SECURING WIRELESS NETWORKS AGAINST EAVESDROPPING USING SMART ANTENNAS

A Thesis
Presented to
The Academic Faculty

by

Sriram Lakshmanan

In Partial Fulfillment
of the Requirements for the Degree
Master of Science in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
December 2007

SECURING WIRELESS NETWORKS AGAINST EAVESDROPPING USING SMART ANTENNAS

Approved by:

Professor Raghupathy Sivakumar, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Mary Ann Ingram
School of Electrical and Computer Engineering
Georgia Institute of Technology

Professor Faramarz Fekri
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: October 17 2007

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

Securing communication in data networks has been a problem of interest since the time of conception of network based communication. With the explosive growth in the usage of wireless data networks over the last several years, increasing attention is now being paid to specifically securing communication in wireless environments. Using air as the medium, while having its obvious advantages centered around tetherless communication, does significantly increase the complexity of challenges pertaining to security. The unique nature of the wireless medium enables an attacker to conduct new kind of attacks such as finger printing and passive eavesdropping without being noticed unlike in a wired context, where interception requires tampering the physical medium. Current wireless security techniques are predominantly cryptographic in nature, where it is typically assumed that the adversary has access to all the information and the techniques are designed to make it *computationally hard for the adversary to understand the true meaning of the information.* Further, such schemes are aimed only at preserving confidentiality of messages, leaving aside several privacy attacks such as fingerprinting. Simultaneously with these developments, sophistication in antenna technology has led to the emergence of smart antennas, which employ signal processing to obtain more degrees of freedom for communication. Some of the benefits of this technology include increased communication range, reliability and performance. In this context, the goal of this work is to *explore how smart antennas can be used to tackle the unique security challenges due to the wireless medium.*

Specifically, the scope of this thesis is restricted to securing communication over wireless data networks, and further limited to a specific form of adversarial behavior - *eavesdropping.* In this context, we define a metric called the *exposure region*

that refers to the area within which an eavesdropper can access and decode the signals being transmitted and first investigate the baseline performance improvements achievable when using adaptive-arrays for beamforming. We show that simple beamforming gives benefits sub-linear in the number of elements and also leaves several common scenarios unprotected. We then propose a suite of strategies that use *arrays of arrays* to provide considerable reductions in the exposure region, called secret sharing, controlled jamming and stream overwhelming. We present the solutions in the realistic context of a *virtual array of physical arrays*, where multiple access points (in the same administrative domain), each equipped with a physical antenna array, are used in tandem to achieve the strategies. Using a combination of *simulations, real-life field trials, and analysis,* we demonstrate the efficacy of the proposed solution.

CHAPTER I

INTRODUCTION

Securing communication in data networks has been a problem of interest since the time of conception of network based communication [14, 16]. The term security, in the context of communication networking, broadly includes several forms including confidentiality/privacy, authentication, availability, non-repudiation, and integrity. With the explosive growth in the usage of wireless data networks over the last several years, increasing attention is now being paid to specifically securing communication in wireless environments. Using air as the medium, while having its obvious advantages centered around tether-less communication, does significantly increase the complexity of challenges pertaining to security. Cryptography based techniques including the wired equivalent privacy (WEP), the wi-fi protected access (WPA), and the 802.11i WPA2 are all examples of techniques that protect wireless communication.

One of the primary properties of such cryptography based techniques is that they *hide the meaning of the information being communicated*, but *not the existence of the information itself*. In other words, it is typically assumed that the adversary has access to all the information and the techniques are designed to make it *computationally hard for the adversary to understand the true meaning of the information*. In this work, we focus on a somewhat orthogonal form of securing communication that is broadly classified into what is sometimes referred to as *physical security*. While the term encompasses a wide variety of techniques, it typically refers to approaches that *limit knowledge of the existence of the information* at the adversary. In other words, the goal is to prevent the adversary from even getting access to the information in the first place. It is imperative to note here that the notion of physical security is by *no*

means a replacement for traditional cryptography, but should be strictly seen as a *complimentary strategy* to better foil the attempts of an adversary.

The scope of this work is restricted to securing communication over wireless data networks, and further limited to a specific form of adversarial behavior - *eavesdropping*. With the growing deployment of wireless data networks, and more specifically wireless LAN (WLAN) hotspots at very high-densities, it is relatively easy for even a casual user to turn into an adversary by eavesdropping on ongoing communication in such a wireless network. This coupled with the fact that increasingly more applications, including ones that would require high degrees of confidentiality such as voice-over-IP, are being used over wireless data networks makes it an important problem to tackle.Specifically, we consider an emerging class of antenna technologies - *smart antennas*, to achieve higher levels of protection against eavesdropping. Smart antennas include a broad variety of technologies ranging from simple switched beam antennas to more sophisticated adaptive arrays and multiple-input multiple-output (MIMO) techniques. Irrespective of the specific technology used, a common defining characteristic of smart antennas is their use of sophisticated signal processing capabilities to achieve better spectral efficiencies, interference suppression, and increased reliability among other benefits. A related property of smart antenna techniques is their *ability to focus communication energy spatially*, thus providing a natural platform to build techniques to provide physical security based strategies to tackle eavesdropping.

In this context, we define a metric called the *exposure region* that refers to the area within which an eavesdropper can access and decode the signals being transmitted[1], and first investigate the baseline performance improvements achievable when using adaptive-arrays for beam-forming. We show that the improvements achievable are sub-linear with k, the number of elements on the antenna-array, and the

[1]We define the metric more formally later in the thesis.

improvements can further be smaller when taking into account scattering in typical indoor environments and link-margins required to tackle fading. Perhaps equally importantly, in high density environments where trusted physical spaces might not necessarily be contiguous, this still leaves a non-trivial region of exposure between the transmitter and the receiver that can be exploited by potential eavesdroppers.

We then propose a suite of strategies that use *arrays of arrays* to provide considerable reductions in the exposure region. The strategies, secret sharing,controlled jamming and stream overwhelming are predicated on two principles to limit an eavesdropper's ability to access and decode information: (i) *spatial diversity*: split and send information over a diverse number of pathways such that an eavesdropper's probability to access all parts of an information is reduced; and (ii) *signal overload*: overload the number of signals or pieces of information accessible at any given point in the network space such that an eavesdropper's probability of being overwhelmed enough to prevent decoding of any part of the information is increased. We present the solutions in the realistic context of a *virtual array of physical arrays*, where multiple access points (in the same administrative domain), each equipped with a physical antenna array, are used in tandem to achieve the strategies. Using a combination of *simulations, real-life field trials, and analysis,* we demonstrate the efficacy of the proposed solution.

The rest of the thesis is organized as follows: Chapter 2 defines the scope for the work and presents background information including the performance when using beam-forming with smart antennas. Chapter 3 presents the three strategies that use virtual arrays of physical arrays to reduce exposure regions and analyzes the performance benefits of each strategy in isolation. Chapter 4 describes the details of the solution including the integrated operations for the three strategies, while Chapter 5 presents practical realization of the algorithms. Chapter 6 presents the performance results using simulations and the field trials. Chapter 7 discusses related

work. Chapter 8 summarizes the thesis with directions for future work.

1.1 Thesis

Thus, the contributions of this work are four-fold:

- We introduce the notion of physical space security in wireless data networks through a metric called the *exposure region*, and study the performance levels achievable when using adaptive-array smart antennas.
- We present a set of strategies that use (virtual) arrays of (physical) arrays to substantially reduce the exposure region, and demonstrate the performance using extensive simulations.
- We also describe an algorithm that synergistically integrates the techniques in the context of wireless local area networks and evaluate the performance achievable using simulations.
- We discuss the practical realization of the approach and demonstrate the benefits using field trials .

CHAPTER II

SCOPE AND MOTIVATION

In this chapter, we describe the scope of the work namely the environment, metric and the assumptions about the eavesdropper. Then, we describe the need for and use of a "physical space security" approach. Subsequently, we describe how beamforming can be applied as a baseline strategy for securing against eavesdropping. We highlight why such a technique is insufficient by itself and summarize the motivations for a better physical space security technique.

2.1 Scope

Here the considerations of the environment and eavesdropper capabilities are described, along with a formal definition of the developed security metric.

2.1.1 Environment

The wireless environment considered is that of a Wireless Local Area Network (WLAN), which consists of p wireless Access Points (APs), each equipped with a k-element antenna array and one or more clients, each equipped with a single omni-directional antenna or an array of upto k-elements. While it is possible that there is a strong Line-of-Sight (LOS) path between the AP and a client, it is also possible to have a rich scattering environment. Further, the degree of fading and the richness of scattering will also vary for different indoor environments. Thus, to begin with, we consider a strong LOS path between an AP and each client. Later, in Sections 3 and 6 we show how this assumption is relaxed to include rich scattering and absence of LOS paths to the clients. We assume that any frequency selective fading is combatted by the use of improved modulation schemes such as Orthogonal Frequency Division Multiplexing

(OFDM) as in current WLAN devices. Further, since the mobility of indoor users is typically low, we do not consider the effect of fast-fading, but consider rapid and variable path loss effects that are typical in an indoor environment. Finally, we assume the clients to be primarily static but consider mobility later in our discussions.

2.1.2 Metric

To quantify the security achieved against eavesdropping, we define a new security metric called the *the total exposure region of the network*, ER_N. This is turn, is defined as the union of the exposure regions of all the clients in the network[1]. The exposure region of the i^{th} client, $ER(C_i)$, is given by the region in which an eavesdropper can decode the information of client i.

$$ER_N = \bigcup_{i=1}^{N_c} ER(C_i) \tag{1}$$

where N_c is the total number of clients in the network. We initially consider a 2-D network, where region refers to area. Note that the above metric applies to both homogenous and heterogenous antenna capabilities (although we restrict our focus only to a homogenous network). Further, the exposure region of a client is also a function of the receiver's (or eavesdropper's) antenna gains. Thus, all references to the metric are for a fixed eavesdropper antenna capability.

2.1.3 Eavesdropper

Our eavesdropper model is captured by the following set of assumptions for the eavesdropper M:

1. M is a wireless node with k antenna elements (where k <= the number of elements at each AP)[2].

[1] A similar but equivalent definition can be given in terms of exposure region of APs.

[2] Later, in chapter 6 we discuss the capabilities required at the eavesdropper to combat the techniques proposed in the thesis, and establish how this condition can be relaxed when all solutions presented are used in tandem.

2. M has access to location information of all the clients and APs.

3. M can perform sophisticated antenna processing with its available elements.

4. APs do not have any information about the position of M or its strategy.

We initially consider the eavesdropper to operate in isolation, but later consider the case of colluding eavesdroppers. We consider both *perimeter security* and *physical security* (*i.e.* security against an eavesdropper situated just outside the physical perimeter of the network or inside the network respectively).

2.2 Adaptive array smart antennas

Adaptive array smart antennas employ an array of antenna elements coupled with both amplitude and phase weighting, thereby making it possible to tune and obtain a large set of angular and spatial patterns. The process of choosing antenna element weights such that the Signal to Noise ratio (SNR) at the receiver is maximized is called *beamforming*. Also, when a strong LOS path is unavailable or multipath is rich, simple beam-steering is less effective and the pattern that maximizes the receiver's SNR does not necessarily have a main beam pointing towards the direction of the client. However, when the weights are appropriately chosen, adaptive arrays work well even in the presence of scattering. Also depending on whether the weight adjustments are performed at the transmitter or receiver, the technique is called transmit beamforming or receive beamforming respectively [6].

Another important feature of adaptive arrays, is their *ability to place nulls in desired directions*. The number of elements on the array is typically called the number of Degrees of Freedom (DOF). With a k element array, it is possible to place $k-1$ nulls in the pattern and use the remaining one DOF for the desired communication. The $k-1$ nulls can be used by a transmitter to restrict the transmitted signals from propagating along unwanted directions and causing intereference, while they

can also be used by a receiver to nullify signals (interference) received in certain directions. Thus, a communication between two nodes equipped with arrays can be made successful by performing one of the above two strategies. However, when more than k streams are received at a receiver, the SNR of all these communication streams is degraded. Although the actual degradation will depend on the power levels, we assume that more than k received streams can cause enough interference to make the communication at the receiver unsuccessful.

In summary, the key properties of adaptive arrays that are relevant to this work are the following:

1. A transmitter can control where it causes interference by the appropriate placement of nulls in its pattern.

2. A receiver can null interference only from up to $k-1$ transmissions. Beyond that, it is unable to decode or resolve the transmissions.

3. It is sufficient for either the interfering transmitter to suppress interference to an unintended receiver, or for that receiver to suppress interference from an unintended transmitter.

4. When more than k parallel transmissions happen within an interference range, all transmissions suffer a reduction in Signal to Interference and Noise ratio (SINR) that will make the signal undecodable.

2.3 Why physical space-security?

While security techniques could be incorporated at different layers of the protocol stack much of the wireless security in the context of WLANs has been above layer 4. i.e the security is typically end to end security. While this kind of software only security might defend against several attacks, it is still insufficient and leaves much room for the attacker. For instance [4] , shows how WEP technique can be broken

in a matter of few minutes and more importantly, even WPA2 with its AES (the latest security technique) can be broken without exorbitant effort. These observations point out that just employing higher layer cryptographic techniques is not sufficient for wireless security. Thus alternative ways are also highly desirable. In this context, the idea of physical space security is to provide security at the wireless transmission level. This is a complimentary approach to higher layer encapsulation/cryptographic techniques. However, it becomes very valuable and desirable in a wireless context due to the following reasons:

1. Tapping the wireless channel is much simpler than a wired channel and as mentioned in [4], all higher layer security techniques (including the latest WPA2) are rendered less effective in a WLAN than in a wired context. The increasing computational power that is available commonly (such as multi-core computing) weakens the protection afforded by techniques which rely on computational complexity. Further, flaws/bugs in the implementation seriously impact the security afforded by higher layer techniques.

2. Higher layer cryptography alone does not attempt to reduce packet interception, because significant additional information such as packet sizes, timing of packets can still be extracted to understand application/protocol behavior and also for user fingerprinting [20]. In such cases, the privacy of users is compromised.

3. Improvements in system design and signal processing now make per packet operations on the transmissions feasible. Such techniques are already performed in some commercial products like 'Ruckus Beamflex' [3] and recommended in the standards like 802.11n. Thus, given these improved capabilities and the inadequacy of current higher layer security techniques, providing security at the transmission/link level becomes highly relevant. Also,many situations already involve directional antennas as a must for the consistent performance and in

such cases an orthogonal security technique will be capacity wasteful, whereas, the physical security would not be so.

4. Finally, physical security being orthogonal to existing securing techniques, wouldn't violate higher layer approaches as it only minimizes interception at the eavesdropper but leaves legitimate clients unaffected.

2.4 A Simple Approach to Enhancing Security using Smart Antennas

Smart antennas have been conventionally used for optimizing different communication parameters such as data rate, reliability, transmission power, increased communication range; etc. In the context of security, the direct relevance of smart antenna capabilities is their ability to beamform and achieve interference suppression to counteract jamming. Specifically, when the directions of arrival of the jammers are known, then it is possible to produce a null in the directions of the jammers. Again, the number of jammers that can be suppressed is utmost $k-1$ for a k element array. Apart from jamming, to the best of our knowledge, smart antennas have thus far not been considered to tackle other security issues.

2.4.1 Mechanism

A straight-forward, simple technique to reduce the possibility of eavesdropping using smart antennas is to employ beamforming. When a transmitter or receiver or both perform beamforming, the signal is contained in a specific region between them depending on the shape of the beam patterns and the antenna gains. But, the exposure region for that communication will also depend on the eavesdropper's antenna capabilities and would increase when an eavesdropper has increasing number of antennas.

In the rest of this section, we study the benefits of such a simple strategy in terms of exposure region reduction, and present approximations for the same.

2.4.2 Benefits

We now analyze how the security benefit (reduction of exposure region) of the simple beamforming mechanism compares to that of a scenario with omni directional antennas. Even with uniform illumination of the array, it is a difficult problem to obtain a closed form expression for the exposure region. Hence, we present approximations for the exposure regions of beamforming using a geometric model and also validate the model and resulting trends using simulations. The scenario we consider is that of a single AP communicates with a single client in the presence of an eavesdropper. To begin with, we consider that the AP has a k element array and both the client and eavesdropper have an omnidirectional antenna. We show later that the resulting trends are similar as long as the client and eavesdropper have comparable antenna capabilities.

Geometrical analysis:

We now use geometrical considerations to obtain an approximate expression for the exposure area of simple beamforming. We consider two approximations for the area covered by beamforming namely the *inscribed parallelogram* and the *sector* as shown in the Figure 1. Let d be the AP-client distance and h the width of the beam in distance units as shown in the figure. The distance d can be measured from the transmission power and the free space propagation laws, given a receive power threshold P_th as follows:

$$d = (\frac{P_t * G_t * G_r * (\lambda)^2}{4 * \pi * P_{th}})^{\frac{1}{\alpha}} \tag{2}$$

where P_t is the transmit power, G_t and G_r are main lobe gains of the transmit and receive antenna and λ is the wavelength used.

The area with a sector model is given by

$$A2 = \frac{1}{2} d^2 * \theta \tag{3}$$

where θ is the null-null beamwidth of the transmitting or receive antenna. For a linear array with k elements and a uniform excitation, it is given by

$$\theta = 2 * sin^{-1}(\frac{2}{k}) \tag{4}$$

As a function of k, the distance can be written as

$$d = c1 * k^{\frac{1}{\alpha}} \tag{5}$$

where $c1 = (\frac{P_t*(\lambda)^2}{4*\pi*P_t h})^{\frac{1}{\alpha}}$. Then the area of the sector approximation $A2'$ is given by

$$A2' = 2 * c1^2 * k^{\frac{2}{\alpha}} * sin^{-1}(\frac{2}{k}) \tag{6}$$

When dividing the omni-directional area by this value, the ratio of exposure regions is given by

$$\frac{A1}{A2'} = \frac{\pi}{2} * \frac{k^{\frac{1}{\alpha}}}{sin^{-1}(\frac{2}{k})} \tag{7}$$

For large values of k, equation 7 can be approximated by,

$$\frac{A1}{A2'} = \frac{\pi * k^{1+\frac{1}{\alpha}}}{4} \tag{8}$$

while repeating the above for the parallelogram case (for small values of α) we get,

$$\frac{A1}{A2''} = \frac{\pi * \sqrt{k^2 - 4}}{2} \tag{9}$$

The error in the expressions is not the same for different values of k and α. The errors were identified by numerical analysis and for the case of $\alpha = 4$, the sector model provides results within 16% of the actual area. This indicates that the exposure area improvement with increasing number of elements grows near-linearly for large number of antenna elements when α is high. On the other hand, for low values of α the benefit is less than linear in k. Since the sector approximation overestimates the region, the benefit is bounded to a linear increase with k. Thus, for most cases of relevance, the benefit grows as a sub-linear function in k.

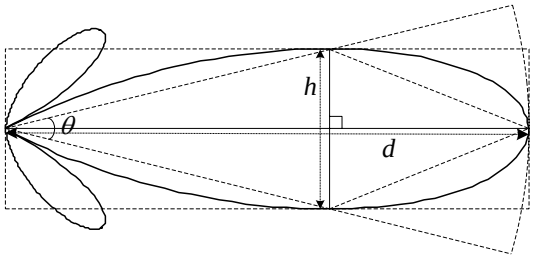

Figure 1: Beamforming area approximation

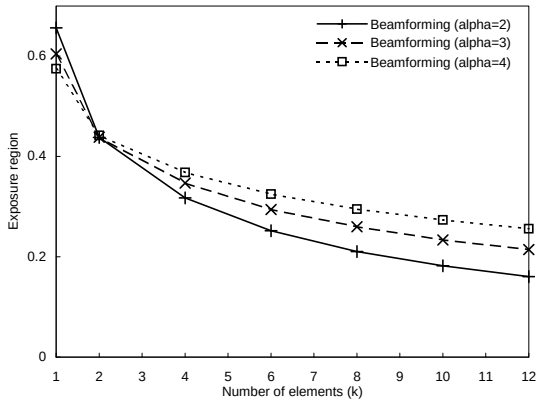

Figure 2: Beamforming benefits

Quantitative analysis:

We now consider the exposure region with actual link margins. Specifically, we study how the benefits vary as a function of the relevant network parameters, namely number of antennas and the path loss exponent. The default values of parameters used are link fade margin of 3dB, 4 antenna elements, and a path loss exponent of 4. We specifically consider two effects, namely the impact of the number of antenna elements and the impact of the path loss exponent. The results are shown in Figure 2. *Impact of k*: When the number of antenna elements is increased, the exposure region decreases. This is reasonable as the beamwidth gets narrower as the number of elements is increased (a $\frac{1}{k}$ dependence as described in [15]). However, more importantly, the decrease rate is less than linear. This means that we get diminishing returns with additional antenna elements. Also it is important to observe that the exposure region has a similar trend as long as the client and eavesdropper have the same number of

antenna elements. This is because, when the AP reduces its transmitted signal power to utilize the antenna gain (for the same received power threshold), both the client and eavesdropper would use their respective gains (same) for reception. *Impact of* α: The path loss exponent also plays an important role in deciding the exposure region. Specifically, Figure 2 shows the variation of exposure region with the path loss exponent. In general, the exposure region increases as the path loss increases. This is reasonable since, a higher transmit power would be required for a larger path loss, so that the received signal power crosses the threshold at the intended receiver. The use of higher transmit power also means that the beam area increases.On the other hand, increasing path loss exponent does not increase the area when the beamwidth is small.

2.4.3 Summary and Motivation

The above results clearly indicate the sub-linear (in k) security benefits possible with simple beamforming, with an example *reduction in exposure region by a factor of half for a six fold increase in antenna elements*. This clearly motivate the need for additional mechanisms for reducing the exposure region and increasing the security benefits. While, beamforming provides a first level security mechanism with a sub-linear k fold improvement, the key question we ask is whether *it is possible for a more intelligent scheme to achieve larger benefits?* In this context, we recall some of the limitations of beamforming: (i) With the higher path loss exponent (typical in indoor environments), beamforming creates a larger exposure region. (ii) Since the benefit with increasing number of antenna elements is sub-linear, the security benefit may not always be sufficient. (iii) It handles only contiguous region security; i.e. adversaries who are outside the common region of the transmitter and receiver, are prevented from receiving a sufficient signal, but if an eavesdropper is present in between the transmitter and receiver, security is compromised. While such security would be

useful for many cases (like an enterprise where entry into the premises is possible only after physical inspection), we argue that it is not sufficient for WLAN environments where the transmitter and receiver can potentially exist in non-contiguous secure spaces. (iv) When a link margin is used (as is typically the case in practice), the area in which an eavesdropper may be able to receive a sufficient signal would be increased.

CHAPTER III

VIRTUAL ARRAYS OF PHYSICAL ARRAYS

In this chapter, we introduce three strategies for improving security in wireless environments using smart antennas that rely on the usage of a *virtual array of physical arrays*. Essentially, inspired by several recent studies about high density access-point deployments ([5, 18]), we exploit the availability of multiple access-points (APs) in a single WLAN environment to form a virtual array. We then assume that each access-point further is equipped with a physical antenna array. We also assume that there are p APs, and they are connected to each other through a high-bandwidth distribution network such as Ethernet. Also, let the c be number of clients, each with 1 to k element arrays.

The three strategies are based on two guiding principles to provide physical space security, namely *prevent eavesdropper from getting access to the information signals* or *overwhelm eavesdropper with more signals than it can sustain such that the information signals cannot be decoded*. Interestingly, the techniques discussed below do apply to a an environment with a *physical array of physical arrays* (a multi-radio smart antenna AP), but exploration of that dimension of the approaches is beyond the scope of this work. Also, while the techniques themselves can be applied to a virtual array of omni-directional antennas, our contention is that the efficacy of the schemes are minimal due to the lack of spatial/angular control with omni-directional antennas.

3.1 Secret Sharing

3.1.1 Overview

The basic idea of secret sharing is well established in the context of cryptography [8]. In a general *t-out-of* n secret sharing scheme, a secret message x should be divided into n shares as

$x \Rightarrow (x_1, x_2, x_3 ... x_n)$ such that the following properties are satisfied.

- **Recoverability:** Given any t shares x can be recovered.
- **Secrecy:** Given any $t' < t$ shares, absolutely no information can be learned about x. More formally, Pr(x|t' shares) = Pr(x)

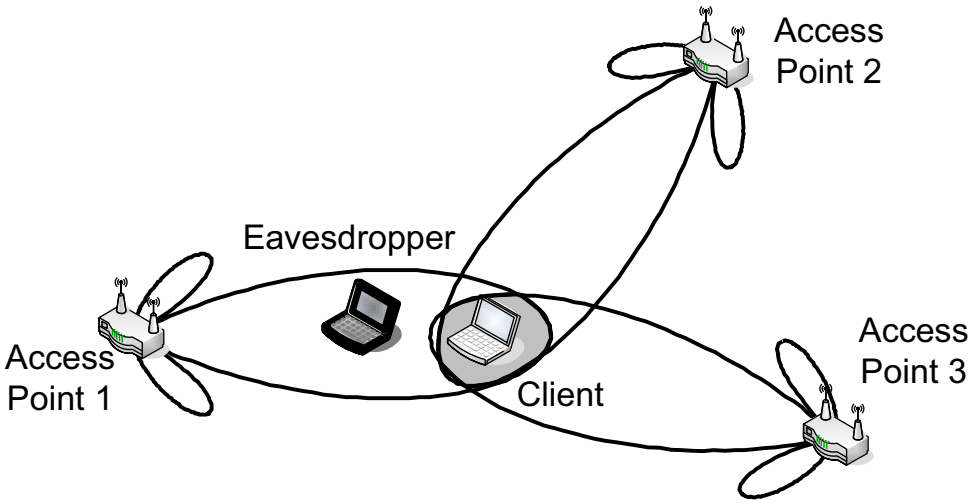

Figure 3: Secret sharing-Illustration

3.1.2 Mechanism

The mechanism exploits the fact that when a single client is reachable from multiple access points, different shares of the message can be distributed to the clients through those access points. An eavesdropper in any position in the vicinity of the client or access points would only be able to gain access to a fraction of the information due to the *spatially disjoint nature of the transmissions* that are possible with adaptive

arrays unlike with omni antennas. Since adaptive arrays allow only one data signal to be received at any time, the multiple elements of the array are utilized to perform beamforming and the scheme is implemented in a time division manner.

Although several secret sharing schemes exist, we are interested in those that do not significantly increase the traffic load on the network given the limited resources in wireless environments. In this regard, we consider the *all or nothing encryption* (as proposed by Rivest [22],) which is a mechanism to prevent parts of a message from being recovered until the whole message was received in its entirety. This method involves encrypting the message with the key, and the key with the message blocks, thus rendering each unusable until the whole sequence (key and message) is correctly received.

A modified version of the above algorithm adapted for a WLAN scenario, is presented here. The mechanism works as follows. Assuming a secure pseudo-random number generator PRNG, which uses a key K of length ℓ bits to generate a pseudo-random sequence PRNG(K). The message that we require to be sent is a bit stream of length $\mid M \mid$. The message M is XORed with the sequence generated by PRNG(K), to create a cipher text C of length $\mid C \mid$, which is the same as $\mid M \mid$. This cipher text is now split into blocks of length ℓ bits. Each of these blocks are now XORed with each other and then with the key K. The result is known as C_ℓ.

Now the controller divides the new packet $C \mid C_\ell$ into fragments of length ℓ bits. All these fragments must be received successfully at the intended client. When the receiver receives these fragments, it XORs all the fragments to regenerate the ℓ-bit encryption key. Once the key is regenerated, the receiver uses it to decrypt the fragments and aggregates them into a single packet based on the fragment numbers. The overhead of such a scheme is ℓ bits for a message of length M bits and provides a strength of 2^ℓ (which means that the overhead increases linearly whereas the number of potential keys increases exponentially.)

We illustrate the scheme using a figure. The figure 3 shows three APs and a single client. Each of the APs possess a share of the information which they communicate to the client in consecutive time slots. Specifically, AP1 transmits its share to the client in slot 1, AP2 in slot 2 and AP3 in slot 3. At the end of the three slots, the client can process the fragments received to decode its packet. On the other hand, consider an eavesdropper who is positioned along the path between AP1 and the client. Such an eavesdropper would be able to obtain share 1. However, share 2 is transmitted from AP2 in the next slot. The eavesdropper cannot receive that share being in the same location because AP2 would perform power control to reach the client with the appropriate power for its decodability but the signal power would reduce quickly before reaching the eavesdropper. The other alternative is for the eavesdropper to move quickly and place himself in the path from AP2 to the client. In this case, the speed with which the eavesdropper must move to reposition himself in the direction of the new path within a time slot, is significant.

3.2 Controlled Jamming

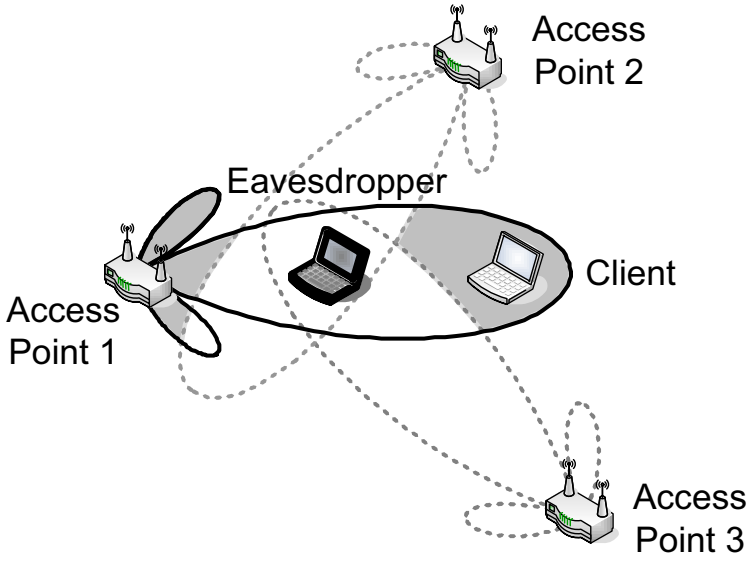

Figure 4: Controlled jamming-Illustration

3.2.1 Overview

The key concept is to generate interfering signals in a controlled manner such that those signals cause no (or negligible) interference at an intended receiver, but cause significant interference to eavesdroppers. In this mechanism, generation of artificial interference is performed by a few "helper" APs. When sufficient interference is generated the signal to interference and noise ratio (SINR) at the eavesdropper is reduced significantly thereby preventing the eavesdropper from obtaining access to the information itself.

3.2.2 Mechanism

The scheme is illustrated in Figure 4, where a single AP attempts to convey a data packet to a client. The other APs in the vicinity generate jamming signals with two constraints: (1) the intended receiver should suffer negligible interference, and (2) the eavesdropper (whose position is unknown) must suffer as much interference as possible. Recall that a k element array can be used to suppress interference of $k-1$ other nodes, if it dedicates one DOF for communication. However, this technique differs from a conventional interference suppression technique in that, a jamming AP does not serve any client and therefore can use all its k DOFs for performing interference suppression and still jam several eavesdroppers. In the figure AP1 communicates a data packet to the client. Simultaneously, AP2,AP3,AP4 generate jamming signals by placing a null in the direction of the client. Then the maximum allowed power is used so that most of the region that is unoccupied by clients is filled with jamming signals. In this way, when multiple overlapping jamming signals are received, an eavesdropper in any of those locations would experience a poor SINR. The eavesdropper can attempt to use its k element array to suppress the interference along the directions of the jamming APs. However, if the number of APs that are in the vicinity is higher than the number of antenna elements, it would still be unable to

receive with a sufficient SINR. On the other hand, the client would be unaffected because the different jamming APs control their beam patterns to place a null in its direction. In this manner, it is possible to achieve protection against eavesdropping by utilizing a set of APs for jamming the adversary. The fine grained control that the k element array provides, enables successful reception at the client while jamming at the eavesdropper simultaneously. It is important to understand that, while increasing interfering transmissions in an omni-directional communication environment leads to higher interference and less throughput, the interference suppression capability is what enables the adaptive arrays to generate jamming signals without affecting the throughput performance of existing flows in the network. Further, the appropriate choice of the power to use depends on the gain in the direction of a null. The power would be limited to be the minimum of the actual power transmission restrictions (as stipulated by the Federal Communications Commission) and the power that is guaranteed to keep existing flows unaffected.

3.3 Stream overwhelming

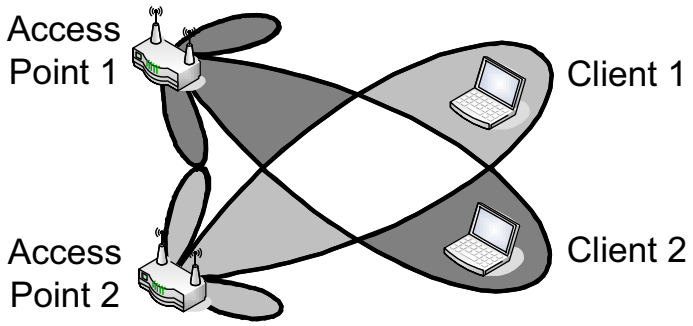

Figure 5: Stream overwhelming-Illustration

3.3.1 Overview

This mechanism exploits the fact that when a node receives more information than the resources possessed to handle it (overwhelmed node), the different information

signals mutually interfere with each other resulting in insufficient SINR for each of these signals. (Here, we use the notion of a stream to indicate each independent data/information flow that a node receives.). Several valid data transmissions are coordinated such that every intended receiver has a sufficient SINR for its desired signal, whereas at other points in the network, the multiple signals interfere to prevent decodability.

3.3.2 Mechanism

Figure 5 shows an illustration of the idea, where two APs and two clients are considered. When each client chooses the nearest AP, then there is no stream overwhelming. However, as in the second part of Figure 5, if the AP client associations are performed in a suitable manner, the beams overlap, causing a larger region to be overwhelmed, thereby reducing the exposure area. We also note here that it is not necessary for the eavesdropper to be present in the overlap of transmission ranges, rather, the eavesdropper would be left with poor SINR even if it is at a point in the overlap of interference ranges. Again in this case, when the eavesdropper attempts to receive from one AP and attempts to suppress interference from other APs, it would still be limited by his degrees of freedom. If the number of APs communicating simultaneously exceeds the number of antennas at the eavesdropper, then it would still be unable to decode the information streams. The stream overwhelming technique is different from a conventional interference suppression strategy in the following sense. Conventional interference suppression aims only at communicating to a node to maximize throughput without a consideration of security. Thus, while the use of adaptive arrays allows multiple parallel transmissions, it is the network-level intelligent choice of the communicating nodes that makes it possible to provide security by exploiting stream overwhelming.

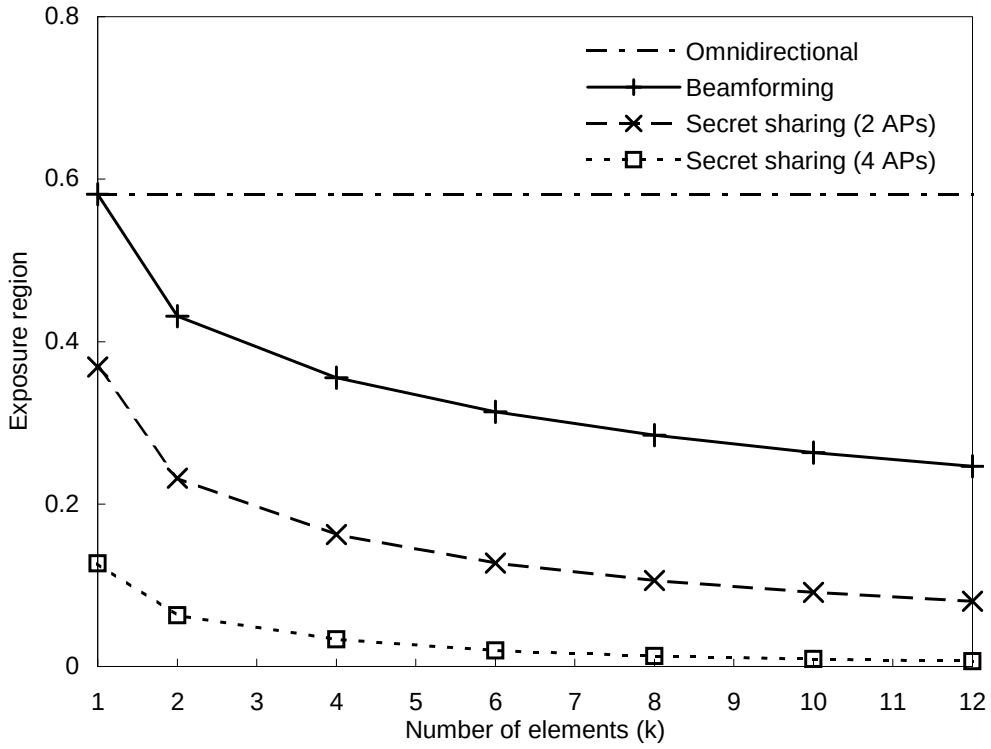

Figure 6: Secret sharing-Impact of k

3.4 Analysis

In this section, each of the baseline strategies is analyzed for their individual performance when the number of antenna elements k and number of APs p are varied. The simulation parameters used in this section are as described in chapter 6. These results are graphically illustrated in the Figures 6,7 for secret sharing, Figures 8,9 for controlled jamming and Figures 10,11 for stream overwhelming. In general, the following observations hold:

• With increasing k, the exposure region reduces.

• With increasing p, the exposure region reduces drastically, in a non-linear fashion.

• When compared to the omni-directional case,for antenna elements ranging from 2 to 12, secret sharing, controlled jamming and stream overwhelming achieve a security improvement of 5x to 37x, 51x to 122x, 3x to 10x respectively.

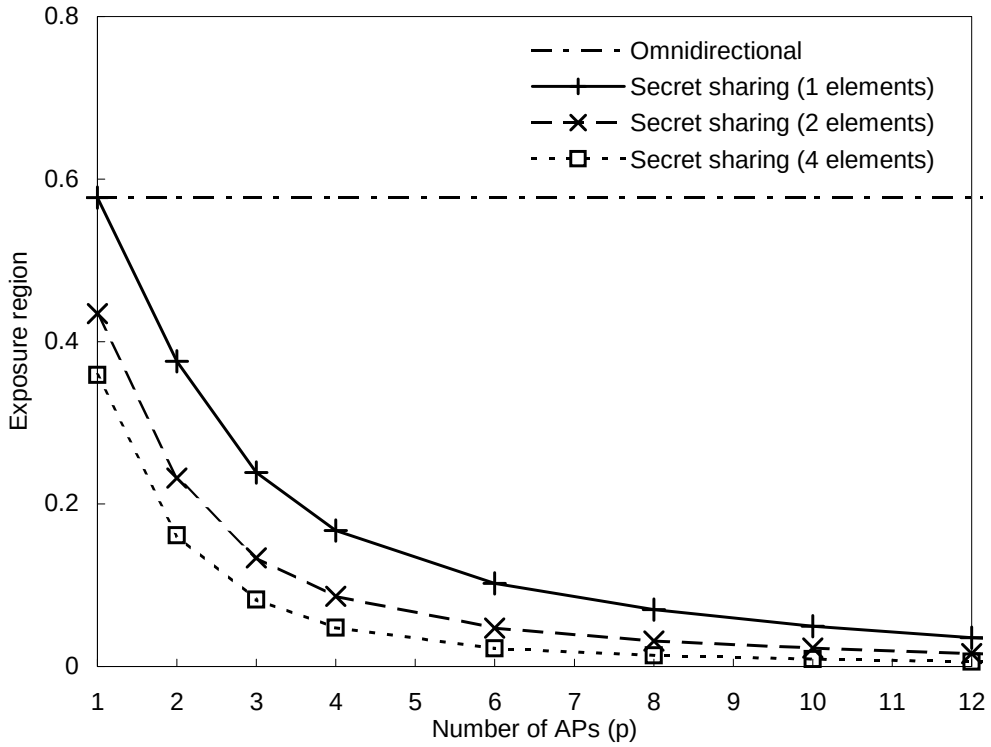

Figure 7: Secret sharing-Impact of p

•Similarly the benefits over beamforming are 3x to 7x, 40x to 54x ,2x to 4x respectively.

•With increasing number of APs, the three schemes achieve,benefits over omni of 4x to 117x, 12x to 260x,2x to 6x respectively and compared to beamforming case, they obtain benefits from 2x to 67x, 8x to 170x,2x to 4x respectively.

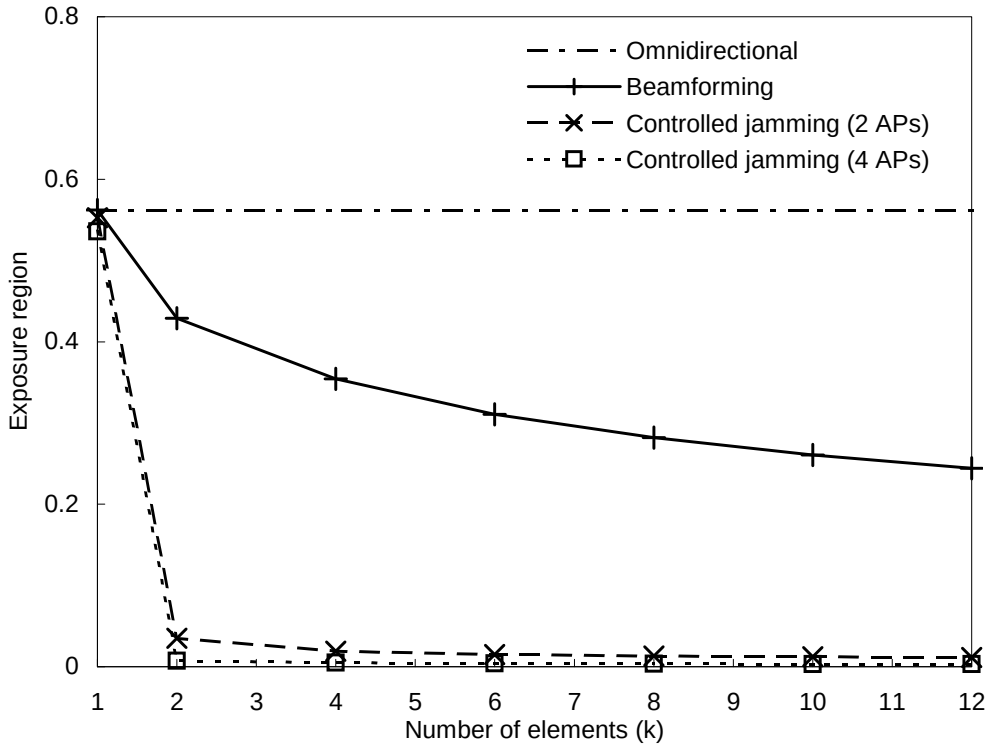

Figure 8: Controlled jamming - Impact of k

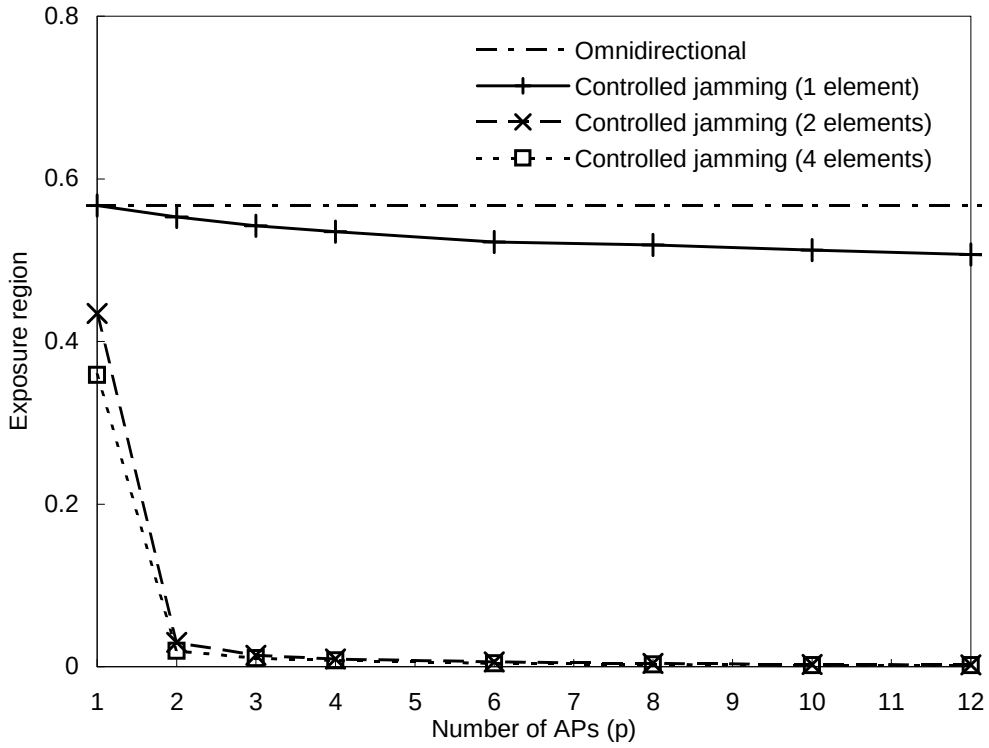

Figure 9: Controlled jamming - Impact of p

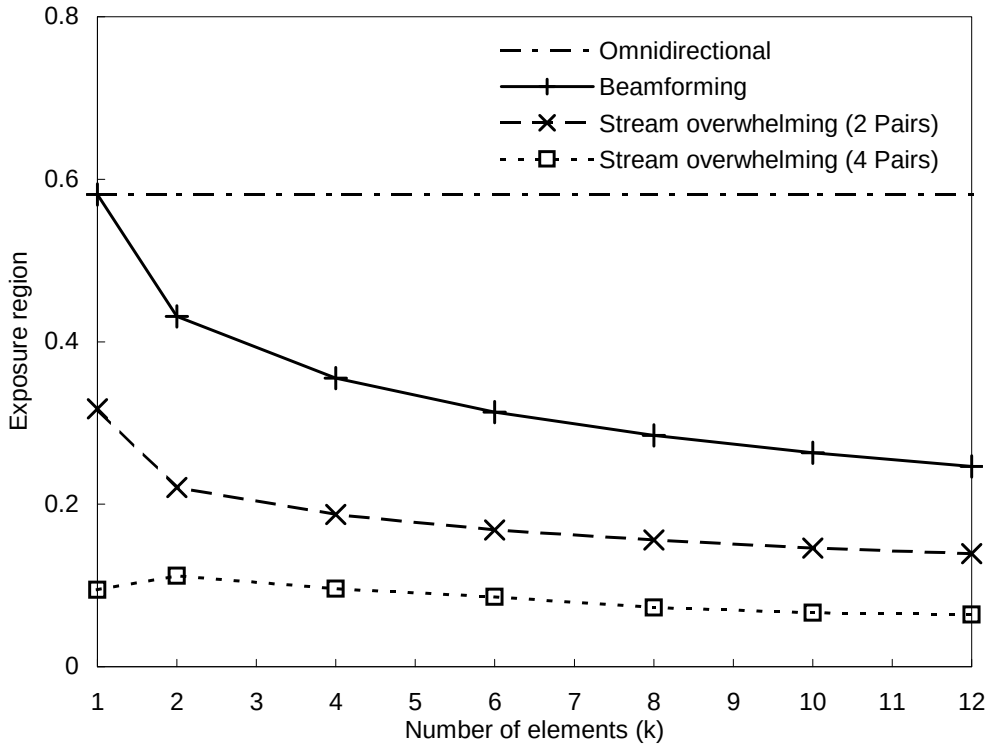

Figure 10: Stream overwhelming - Impact of k

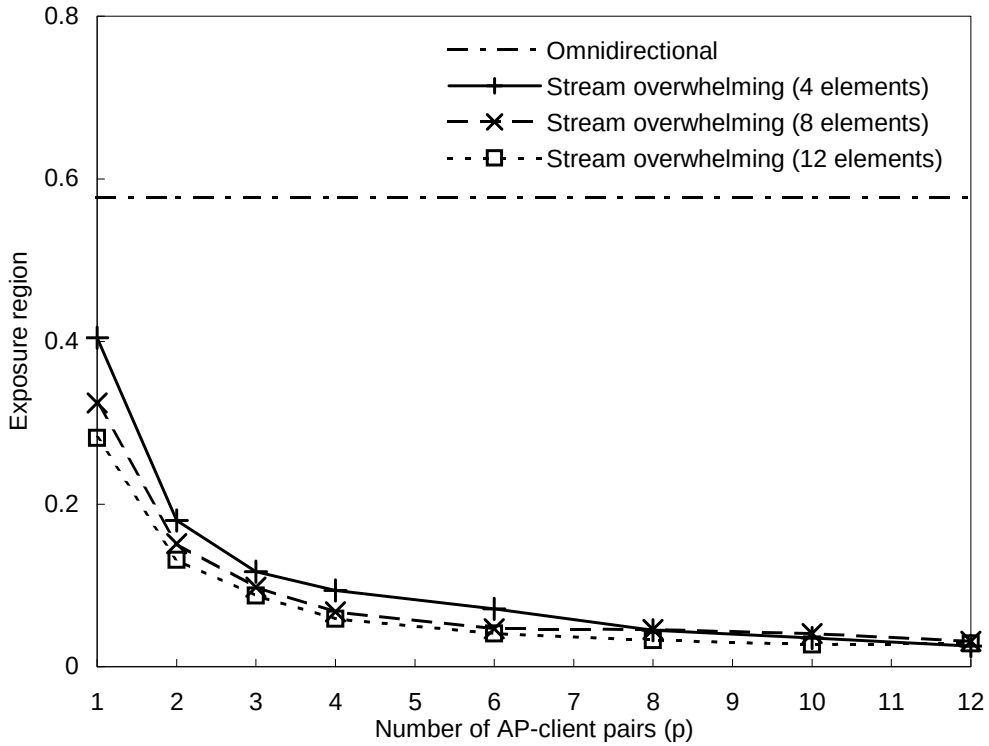

Figure 11: Stream overwhelming - Impact of p

CHAPTER IV

ARCHITECTURE AND ALGORITHMS

This chapter describes the architectural and algorithmic aspects of the proposed solution. Specifically, the network model is described along with the considerations that are required to successfully integrate the strategies developed in the previous chapter. The problem formulation is then described followed by a description of the main algorithms.

4.1 Architectural Model

The architectural model that we consider consists of a central controller connected to several access points as shown in the figure 12. The controller receives from the backbone a stream of packets to be transmitted over the wireless LAN to the clients. For such packets, it employs a combination of the schemes discussed in Section 3, and forwards the packets to the appropriate access-points. We assume that the controller has strict synchronization and control over the access-points. All transmissions by the APs are done at the granularity of *synchronized fragment slots*, where the length of a fragment slot is smaller than that of a *packet slot*. The controller controls both the downstream and upstream (we discuss upstream communication toward the end of the section) modes of communication, and the two modes alternate in epochs. For downstream communication, the controller divides packets into fragments, applies its security decisions, and provides the APs with a set of fragments to transmit.

4.2 Integrated Operations

While we discussed the three key strategies of secret sharing, controlled jamming, and stream overwhelming in Section 3, an important element of the operations is *how are*

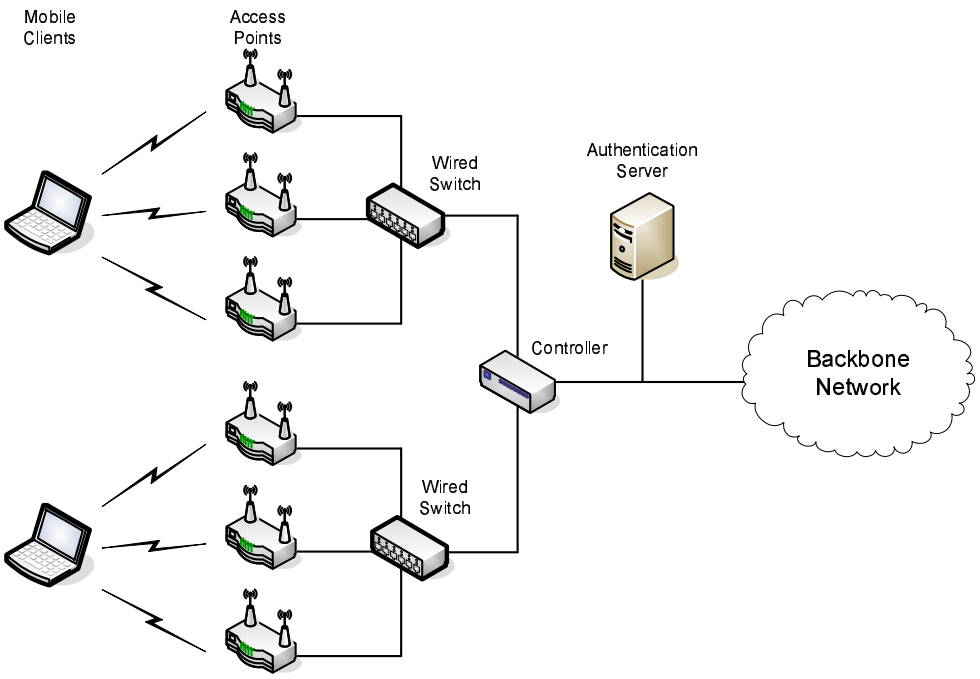

Figure 12: Network Model

the three techniques used in tandem to achieve the best performance possible? While we present the details of the integrated operations in the description of the algorithms later in the section, we now briefly discuss the important constraints and trade-offs that form the basis of the algorithmic design. Briefly, two types of considerations need to be taken into account in deciding on the specific form of integration between the three techniques:

- *Security vs. throughput:* The primary trade-off in using the VAPA techniques outlined thus far for security is in the form of throughput. However, the three techniques differ in the extents of the trade-offs. Stream overwhelming provides its security benefits *without any degradation in throughput.* controlled jamming, on the other hand, uses access-points (other than the primary sender) purely for generating interference, and hence trade-off throughput the most. Finally, secret sharing can achieve certain levels of security without trading-off throughput, but can also trade-off throughput further to achieve a higher level of security. Hence,

from a *security - throughput trade-off standpoint, controlled jamming performs the best for security, but the worst for throughput. Stream overwhelming does exactly the opposite, while secret sharing lies in the middle.* Thus, for any set-up with security objectives with throughput constraints, the above trade-offs will have to be taken into account while determining the extent to which each of the three techniques will be used.

- *Network resources and topology:*

  Another important set of influencing factors includes the number of elements at the APs (and clients), the number of APs, and the specific topology. For example, if a client is accessible only through one AP, it cannot receive any secret sharing benefits. Stream overwhelming benefits can be achieved as long as AP-client pairs within interference range of each other are scheduled to transmit together. Finally, controlled jamming can be accomplished as long as there is one or more APs within interference range of a scheduled transmission. From a number of resources standpoint, secret sharing depends more on the number of APs, whereas controlled jamming and stream overwhelming depend more on the number of elements on the APs.

Based on the above considerations, it is clear that the desired throughput-security values and the available network resources and topology determine the right choice of strategies. Hence, the main guiding principles adopted for the algorithm design are as follows: (i) For a desired security, if capacity has to be maximized, then one must determine whether the security is achievable by purely stream overwhelming or secret sharing alone. If not, then the minimal number of APs necessary for controlled jamming needs to be used such that it will guarantee the desired level of security, and use the remaining APs for secret sharing or stream overwhelming to improve security while maximizing the capacity. (ii) Similarly, for a desired throughput constraint,

if security has to be maximized, a combination of stream overwhelming and secret sharing (with preference to secret sharing) should be used for achieving the desired throughput, and the remaining APs should be devoted to controlled jamming to maximize security.

In the rest of the thesis, we consider only the model where subject to a throughput constraint, security needs to be maximized. All discussions can be extended with minimal effort for the alternate model as well.

4.3 Problem Formulation

In the model described thus far, the intelligence is concentrated at the controller and can be divided into two major components, *the throughput scheduler and the security scheduler*. The throughput scheduler takes as input a throughput constraint S and determines the maximum number of packets j that are schedulable subject to a bound of S. This value j is then fed into the security scheduler that then determines the right strategies to use to maximize security while transmitting the j packets.

The problem formulation for the two components is described below. Consider that the controller has an infinite stream of packets in its queue. We assume that any fairness mechanisms are implemented even before the packets reach the controller. In this fashion, the security algorithm works without affecting the fairness and is agnostic to the fairness mechanism used. The algorithm serves packets only in the order that they were queued to prevent potential starvation and out-of-order delivery problems . The throughput constraint fed to the algorithm is S, the minimum number of packets to be transmitted during a slot (if schedulable). The objective of the algorithm is then to determine the AP actions for each fragment duration in-order to maximize the number of consecutive data packets that can be scheduled subject to an upper bound of S. Once the number of consecutive data packets is determined, then the algorithm tries to maximize the security benefit.

The formulation is presented in figures 13 and 14.

Given $G(V, E)$,
$V = M \cup N$: set of vertices
M: set of APs
N: set of clients
E: set of edges
$w_{ij} = \begin{cases} 1 & : \text{ input packet stream} \\ 0 & : \text{ otherwise} \end{cases}$
K: number of elements on each AP
Given P_s,
$1 \leq s \leq S$: input packet stream
$n(P_s) \in N$: destination client of packet P_s
Output:
Mapping from S' packets to APs
$m(P_s) \in M$, $1 \leq s \leq S'$
Solution:
Maximize S'
Subject to:
(1) Each AP sends at most one packet
$m(P_s) \neq m(P_t)$, $s \neq t$, $1 \leq s \leq S'$, $1 \leq t \leq S'$
(2) Each client receives at most one packet.
$m(P_s) \neq m(P_t)$, $s \neq t$, $1 \leq s \leq S'$, $1 \leq t \leq S'$
(3) Each active AP has at most $k-1$ interfaced active clients.
$\forall s$, $1 \leq s \leq S'$,
$\sum_{t=1, t \neq s}^{S'} w_{(m(P_s), n(P_s))(m(P_t), n(P_t))} \leq k-1$

Figure 13: Throughput scheduling optimization

The first part in the formulation is to determine the number of in-sequence packets j that can be scheduled out of the first S packets. S is thus a tunable knob which can be used to tune the desired levels of security in the network. For instance, if $S = 1$, then the problem reduces to maximizing security for this single packet's transmission. However, when S is larger (bound by the number of APs) then throughput is maximized, and any security achieved is opportunistic using unassigned resources. Note that, given a set of S packets, the number of in-sequence packets that are schedulable is not fixed but depends on the way APs are assigned. Thus the largest number of packets that can be scheduled will be achieved for the optimal scheduling algorithm. In the second part of the problem, the security mechanisms need to be applied to

Given P_s,
$1 \leq s \leq S$: input of schedulable packet stream
Output:
Mapping from S' packets to F fragments to APs
$m(P_s, f) \in M$, $1 \leq s \leq S'$ $1 \leq f \leq F$
Solution:
Minimize $max(ER(P_s))$
Subject to:
(1) Each AP sends at most one packet in one fragment.
$\forall f$, $m(P_s, f) \neq m(P_t, f)$, $s \neq t$, $1 \leq s \leq S'$, $1 \leq f \leq F$, $1 \leq t \leq S'$
(2) Each active AP has at most $k-1$ interfaced active clients.
$\forall f, \forall s$, $1 \leq f \leq F$, $1 \leq s \leq S'$,

$$\sum_{t=1, t \neq s}^{S'} w_{(m(P_s,f),n(P_s))(m(P_t,f),n(P_t))} \leq k-1$$

Where:
Exposure region of packet P_s:

$$ER(P_s) = \bigcap_{1 \leq f \leq F} ER(P_s, f)$$

Exposure region of packet P_s in fragment f:

$$ER(P_s, f) = \{(x, y) \in R^2 | SINR(x, y, i, f) \geq \text{threshold}\}$$

SINR of packet P_s at (x, y) in fragment f:

$$SINR(x, y, P_s, f) = \frac{\frac{W_{m(P_s,f)} \cdot G_{m(P_s,f)}(x,y)}{\{d_{m(P_s,f)}(x,y)\}^{\alpha}}}{Noise + \sum_{t=1, t \neq s}^{S'} \frac{W_{m(P_t,f)} \cdot G_{m(P_t,f)}(x,y)}{\{d_{m(P_t,f)}(x,y)\}^{\alpha}} + \sum_{i \in FA_f} \frac{W_i \cdot G_i(x,y)}{d_i(x,y)}}$$

W_i: transmission power of i-th AP
$G_i(x, y)$: gain of i-th AP toward (x, y)
$d_i(x, y)$: distance from i-th AP to (x, y)
α: path loss factor
FA_f: free APs in fragment f
,where $FA_f = \{i \in M | m(P_s, f) \neq i, 1 \leq s \leq S\text{`} \}$

Figure 14: Security optimization

the j in-sequence packets such that those j packets are transmitted by the end of the slot but the security is maximized for these j packets. The problem is thus concerned with appropriate choice of strategies for the APs during the fragment durations of this slot.

4.4 Idealized model and algorithms

The idealized model for the application of the proposed security solution, as described earlier, consists of a central controller which controls the communication actions of each of the access points. In such a case, the access points have a high degree of

synchronization and do not take independent actions. Further, the access points act exactly as dictated by the controller. The controller is also assumed to have access to the head of line packet of the queue in each access point and thus has complete command over what packets get transmitted on the wireless network at all time. The controller is also assumed to know the positions of the access points and clients in the network. We focus only the downstream communication here, and revisit upstream communication later in the section. We now present the details of the two cascaded schedulers at the controller.

4.4.1 Throughput Scheduler

The throughput scheduler takes as input the control parameter S and the first S packets in the input queue of the controller. It provides as output the set S' of the j schedulable in-sequence packets. The algorithm used is a greedy algorithm that attempts to maximize j, the number of insequence packets that would be served during this transmission slot considering the spatial reuse and the adaptive interference suppression capability.[1]. The working of the algorithm can be understood by observing the pseudo-code.

The throughput scheduler first calculates how many clients for this packet stream can potentially use an AP, for each of the APs in the AP set M (lines 1-2). Then, for each packet starting from the first packet in the queue, the set of available APs is computed (line 4). Of this set, the one with minimum potential clients is chosen to be the one for this packet (line 5-7), as long as there is some such AP. Then the available APs, DOFs at each APs, and the number of potential clients are updated at each AP. In this fashion, the number of schedulable packets in sequence is given by the number of packets that could be assigned.

[1]Note that while we use a greedy algorithm as a representative, any throughput scheduling algorithm designed for adaptive arrays is usable at this stage.

S': schedulable number of packets
PS: schedulable packet stream
PS_s: first s packets in the packet stream
p_l: l^{th} packet in PS
F: number of fragments
$r(a, b)$: available DOF of AP a for fragment b
f: fragment index
E: network Connectivity matrix
$AP(n)$: set of APs within communication range of client n
$n(p_i)$: destination(client) id of packet P_i,
W_{ij}: (i, j)-th element of link conflict matrix,
$W_{(ab)(cd)}$: link conflict indicator between links ab and cd,
$m(p, f)$: assigned AP id of packet p during fragment f
$Action(a, f)$: action of AP a for fragment duration f
N: set of clients for which packets are destined in PS
M: set of APs which are in range of clients in N

Figure 15: Definition of variables

4.4.2 Security scheduler

The objective of the security scheduler is to identify the assignment of actions of APs for different fragment durations such that all the packets handed down by the throughput scheduler are scheduled, while minimizing the exposure region. These are performed in a greedy manner, where secret sharing is the default strategy. However, when there is a tie between two choices of available APs for a fragment, both giving the same secret sharing benefit, then stream overwhelming is used as the strategy of choice. Once the possible fragments are scheduled (i.e the throughput scheduler's constraint on number of packets is met), controlled jamming is attempted in the free fragment durations. The free APs determine if the number of clients, for which to perform interference suppression, is less than k-1. If so, that AP performs jamming for that fragment duration, otherwise, the next free fragment duration is checked.

The pseudocode describes the mechanisms. Particularly, the edge connectivity matrix is given as E, where an entry of 1 in the $(i, j)^{th}$ position indicates that node i and node j are within communication range of each other. The link conflict matrix is given as W, where W_{ij} is 1 if the links i and j are interfering links. Similarly $W_{(ab)(cd)}$

```
Greedy_Throughput() :
    INPUT: S, PS, m(Ps), E, W
    OUTPUT: m(Ps)
1   For each a in M
2   NC(a) = Calculate_Number_of_possible_clients
3   For each value s from 1 to S
4   APS(s) = Calculate_available_APs(n(Ps))
5   MAP = Find_Minimum_NC(APS)
6       If MAP≠ NULL
7           m(PI_j) = MAP
8           Increment assigned
9           Update_Available_APS
10          Update_Available_DOF
11          Update_NC
12      S' = assigned
```

Figure 16: Throughput scheduler

represents whether links ab and cd interfere with each other. The algorithm takes as input the set of schedulable packets provided by the throughput scheduler, the connectivity and interference matrices of the network, and the set of client destination ids of the packets. As output, the algorithm provides the actions of the different APs for the different timeslots. This is indicated by $Action(a, f)$ to indicate the action of AP a during fragment duration f. The action can either be a transmission of a fragment to a client c (indicated by $Action = c$ in the pseudocode) or controlled jamming with care about clients (indicated by $Action = JAM$)in the vicinity. Based on this, the APs to which each fragment of each packet is destined ($m(ps, f)$ in the pseudocode) can also be obtained.

To begin with all the APs reachable from a client are included in the list of available APs for each client. Then the packets are arranged in ascending order of the number of APs(line 8). This is because clients with fewer number of APs should definitely be scheduled and must not lose their AP to other clients who may want to perform secret sharing. The next step is to identify the availability of each of the APs of the client under consideration for the different fragment durations (lines 11-13). Specifically,

Initialize() :

1 For each m in M
2 For $1 \leq f \leq F$
3 $r(m, f) = k$
4 For each n in N
5 $AP(n) = \{m \in M | (m, n) \in E\}$
6 $PI = PS$

Security :

INPUT: S', PS, $m(Ps)$, E, W
OUTPUT: $Action(Ap, f)$, $m(Ps, f)$
7 Initialize()
8 sort_ascending(Pi,NUM_APS)
9 For each packet i from 1 to S'
10 $n = n(p_i)$
11 For each fragment f
12 For each AP m
13 $Avail(m, f)$ = Determine_availability(m,n,f,i)
14 $APList$ =Sort_ascending(APs,fragment_num)
15 Adjust_stream overwhelming(APList)
16 For each AP in APList
17 $fragment$ =Select_random_availablefragments
18 $Action(AP, fragment) = n(p_i)$
19 For each free AP a
20 For each free slot t
21 $Action(a, t) = JAM$

Figure 17: Security scheduler

the number of fragment durations that each AP is available and which of the fragment durations each AP is available. The availability of an AP during a fragment is decided by the number of already scheduled active clients in its vicinity and the number of DOF that it possesses. For instance, if there are already k-1 scheduled transmissions in the vicinity of this AP for that fragment duration, then any additional transmission would surely cause interference. Next, the available APs are sorted in ascending order of the number of slots in which they are available. The AP with the fewest available fragments is scheduled first because, the allocation tries to greedily assign different APs for the fragment durations to obtain the secret sharing benefit. For instance, if an AP is available for only one fragment duration and another available AP is

allocated during that fragment, then this AP would not be included(reducing the secret sharing benefit). Lines 15-18 describe the AP allocation. The APs are allocated in a round robin manner such that for each AP one of the available fragment durations is picked randomly. Such a technique has an advantage over randomly selecting one of the available APS for each fragment duration. This technique ensures that as many different APs are chosen as possible, whereas in selecting one of the available APs randomly for each fragment, there is a finite probability that a single AP is chosen for all fragments minimizing the secret sharing benefit. The algorithm thus ensures that the secret sharing benefit is maximized greedily. Here, when there are more than one APs with same number of available fragment durations, the choice of AP is such that stream overwhelming is possible (Line 15 indicates this).

Once the data schedules are completed, the controlled jamming strategy is applied (lines 19-21). For all the free fragment durations, the number of scheduled clients in the vicinity of that particular AP for that duration is determined. If this value is lesser than k-1, then it is possible to perform controlled jamming without interfering with legal clients and the AP is assigned a jamming action. However, if there are already enough clients in the vicinity, then controlled jamming would not be applied. In this way, the algorithm greedily applies the techniques according to the design guidelines presented in the previous section.

CHAPTER V

PRACTICAL REALIZATION

In this chapter, the issue of practicality is discussed. First, it is described how, using currently existing standards a solution can be constructed without significant modifications. Further, the systems related requirements are listed , along with pointers about their current existence in the industry.

5.1 Protocol and standards

We now briefly discuss an approach for practical realization of the strategies discussed thus far in the context of the 802.11 PCF (point coordination function) mode of operation. The 802.11 PCF is an access mechanism that operates in the infrastructure mode, where an access point of a cell acts as the central coordinator called the Point Coordinator(PC). The PC grants a contention free channel access to individual nodes by polling them for transmissions. On being polled, a node transmits a single frame. In the infrastructure mode, time is divided into periodic superframes which start with the beacon frames. At the beginning of a superframe, the PC waits for a PCF Inter Frame Spacing (PIFS) for the channel to be idle and then transmits the beacon frame which is a broadcast packet carrying special information. The PC, then consecutively polls each of the stations that operate in PCF mode, one at a time. At the end of the CFP, the PC sends a CF-END frame to signal the end of that CFP.

The PCF mode of operation is well-suited to the proposed solution in the context of a virtual array of physical arrays. The polling based mechanism endows the PC with the exact transmission slots for each client's communication. The controller can assign the sequence to be used by each PC. Since the controller acts as a central decision maker, the exact assignment of actions to each AP in the network is possible and is

accomplished within the current framework of the WLAN PCF mode of operation.

However, since transmissions are arranged always in an "AP first, client-next manner", the actions of the APs for the durations of the client communication must also be determined. Specifically, since each AP listens for the reply from a client, it cannot be utilized to perform other actions such as counter jamming. Hence, when the clients talk, the counter-jamming APs must now perform interference suppression with respect to the APs and not the clients. In this fashion, the existing solution can be adapted to take the direction of information flow and the slotted access within the PCF mode of operation.

While the basic security solution has been presented in the context of downstream communication, it is relatively straightforward to extend the schemes to the *upstream communication* as well. To make correct decisions, it is necessary to obtain information about the time slot that different clients would use for their transmission. However, the use of a polling based mechanism, enables the AP to know what time duration a transmission can be expected from a client. This information is used along with the client positions to generate different communication patterns. More specifically, the controller performs centralized control to determine the actions of APs for the downlink, whereas the polling to cater to the clients and provide upstream security can be obtained by the APs controlling the polling sequence. This would enable the controlled jamming technique to be applied with the modification that nulls are placed by the jamming AP towards other APs in the vicinity as opposed to clients. However, stream overwhelming could be performed by adjusting the polling sequence. Also, the secret sharing approach can be applied by the client transmitting fragments to different APs consecutively. This will require that the client be able to obtain a dedicated fragment duration to transmit to each of the APs. In this manner, the basic schemes are applied with modifications of parameters.

5.2 System requirements

The following paragraph is used to illustrate the main system design issues that need to be addressed to make the overall solution practical. (1) Beamforming weight determination: When a node needs to beamform to another node, the antenna weights for the other node must be available. This can be obtained using standard pilot symbols or preambles. Such an approach is already employed in cellular systems and also in upcoming standards like IEEE 802.16 [2], IEEE 802.11n [1] (2) Weight adaptation resolution: When the client node mobility is limited, the beamforming weights need to be adapted , in order to form an accurate beam towards the desired client. (3) Beam setting time: The time required to actually set the beam and for the antenna to settle, is an important system consideration. While the actual setting time depends on the exact system detail, setting at packet granularity is already accomplished in some commercial products [3].

CHAPTER VI

PERFORMANCE EVALUATION

This chapter evaluates the proposed solution using simulations and field trials and establishes the magnitude of benefits achievable for different network conditions.

6.1 Simulation Model

The simulations were carried out using a custom simulator written in C++. The custom simulator incorporates the following modules: smart antennas pattern computation [15], ability to perform adaptive array processing [21] and indoor channel models .

The details of the models are :

- Beamforming: Simulation support is developed for generating a desired beampattern and also to perform adaptive interference suppression using the techniques described in [21].

- Channel model: For the channel model, various models were implemented to account for the indoor propagation law. Specifically, the ITU model was used. This model accounts for the variation in power levels and fading.We also consider the ITU model for indoor attenuation and a link margin of 3.2 dB (3dB with a 90% link reliability). We consider an operating frequency of 2.4 GHz, an SNR threshold of 15 dB and a noise level of -100dBm (0.1pW). Further , we use a sensitivity of -85dBm (3 pW) and a maximum transmission power of 20dBm (100mW) as used in standard 802.11 equipment . The default values of parameters are : number of antennas is 4 and number of APs is 4.

- Positions: The position of the client and AP positions are generated randomly within the grid of points in a 100m * 100m grid. Such a grid size was chosen to incorporate the fact that indoor ranges are much smaller than actual free-space ranges. The position of the client is also chosen randomly within this grid. The eavesdropper's position was also selected randomly within the grid. The default number of clients chosen is set as 20.

- Traffic flow: Downstream flows are setup to a randomly chosen subset of clients. The number of clients selected is decided by the selection parameter S (described in Chapter 5) and the output of the algorithm. The default value of selection parameter is the same as that of the number of APs.For each data point, the average of 20 simulation runs is calculated.

- Metric: Here the metric of interest is given by the exposure region as defined in section 2. When multiple clients exist in the network we consider two metrics , namely the average exposure region of the clients over different client positions and the maximum exposure region of any client over different client positions.

6.2 Simulation results

The exposure region for the integrated algorithm is described in the following, as the parameters are varied.

1. Varying number of elements k:

In this part, we explore the effect of varying the number of antenna elements on the APs.From Figure 18 and 19, as the number of elements on the APs is increased, the exposure region is reduced in both the average and worst case scenarios. We also observe that the exposure region is extremely small when the integrated algorithm operates. Further, and more importantly, the exposure region of simple beamforming is much larger compared to the integrated solution. This means that it is only the intelligent use of the mechanisms that gives large security gains and not just simple

beamforming. Further, the throughput also increases with increasing k.

2. Varying number of Access Points p:

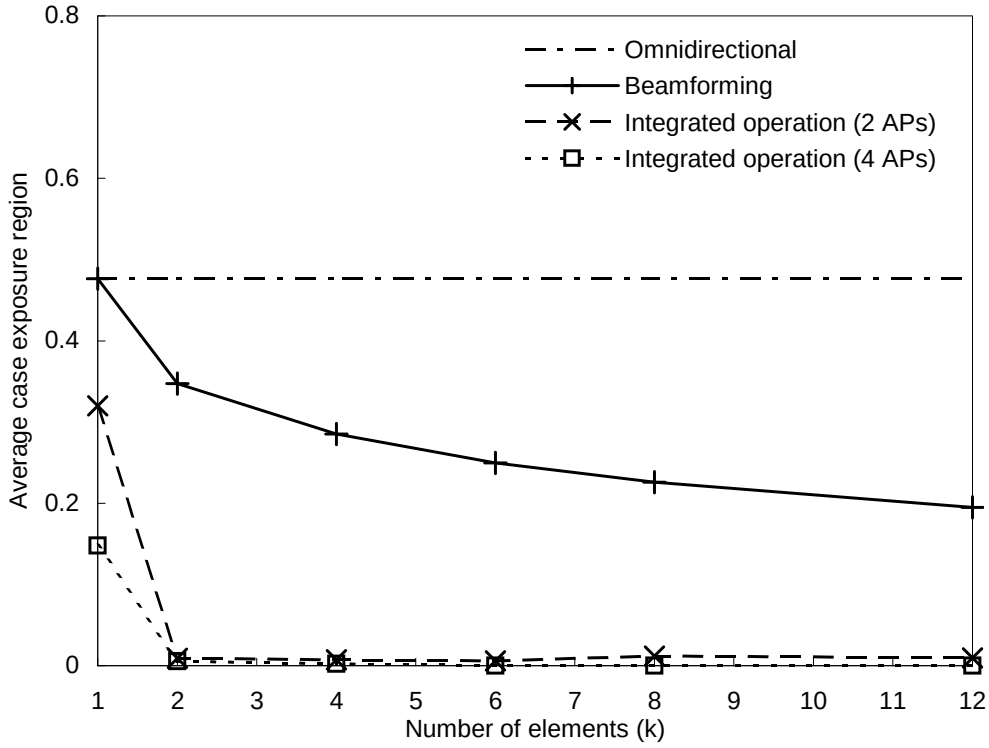

Figure 18: Impact of k - Average exposure region

Figures 20 and 21 plot the average and worst case exposure region as the number of access points is varied. We observe again that the exposure region reduces drastically as the number of APs is increased. Specifically, with 12 APs, a 2000x improvement is possible when a single eavesdropper is considered.

3. Varying value of tuning parameter S and throughput:

The results for varying S values is shown in Figures 22 and 23 for the average case and worst case respectively. As the value S is varied from low to high, the importance shifts from security to throughput. The figures show that security value does not degrade significantly as the value of S changes from low to high. This means that although the throughput is optimized, the security is not degraded significantly

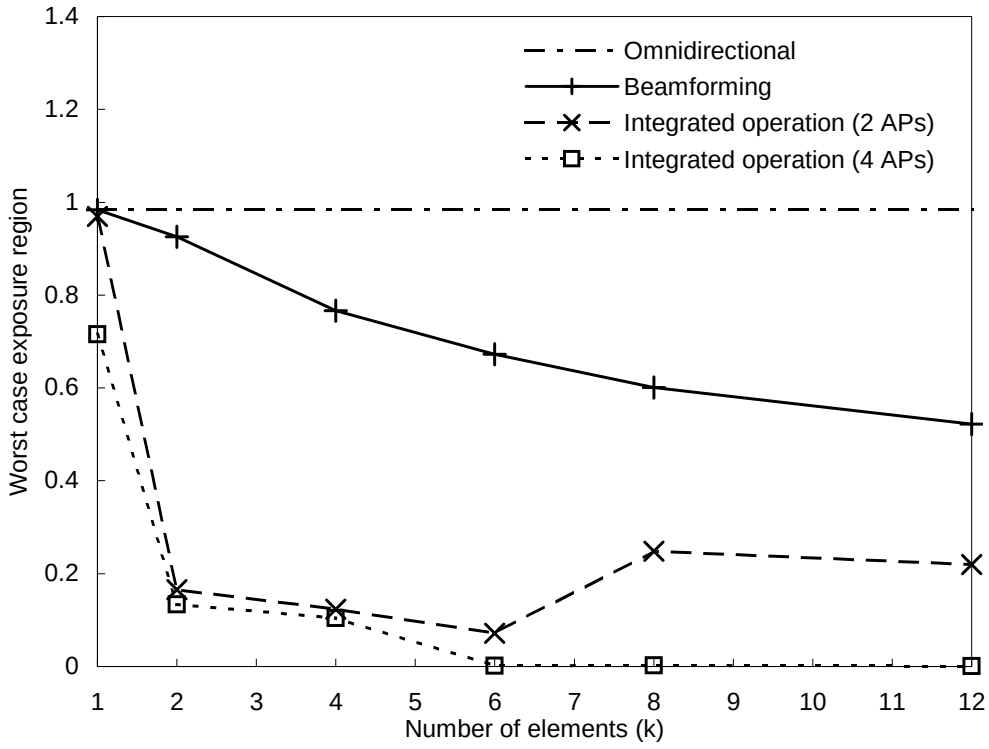

Figure 19: Impact of k - Worst case exposure region

for the given network conditions. However, we observe that while the throughput increases with increase in S, the security benefit does not degrade. This is counter-intuitive and means that the stream overwhelming benefit also increases when the number of scheduled transmissions increases. This suggests that the intelligent use of all the three techniques enables maximizing both throughput and security without any significant trade-off.

4. Varying number of colluding eavesdroppers:

Here, we simulate the effect of colluding eavesdroppers as follows. For each packet destined to a client, we calculate if at the end of the slot duration, the eavesdroppers together have all the fragments for a client's packet. Here the metric of exposure region by itself is not sufficient. Hence the metric used here is the packet exposure

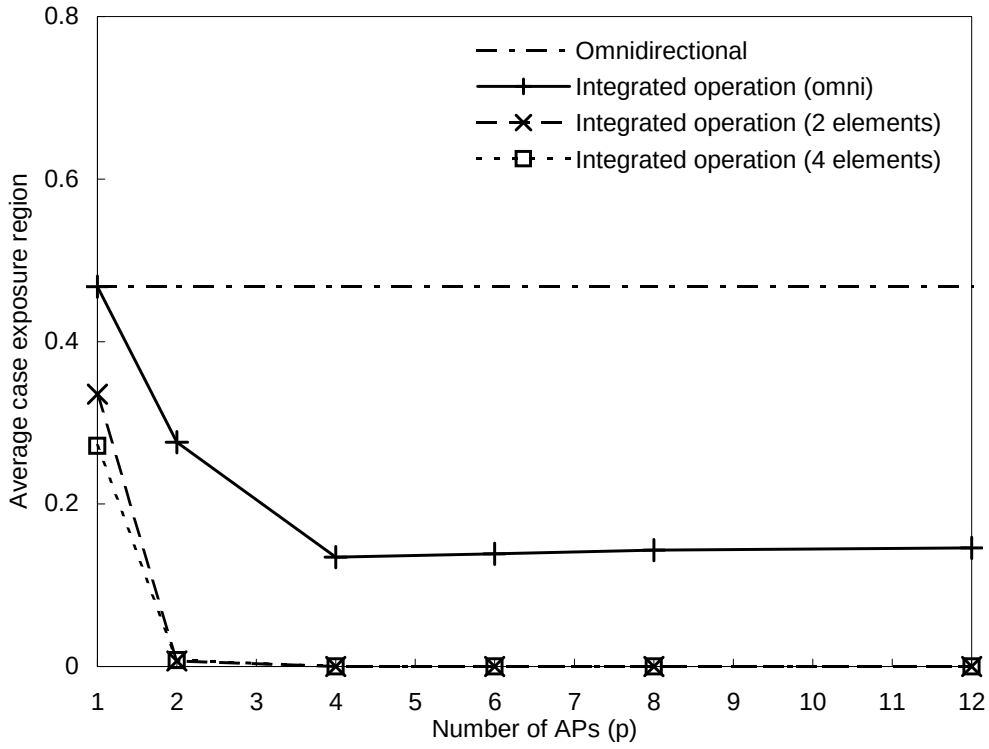

Figure 20: Impact of p - Average exposure region

ratio. Packet exposure ratio for a given scenario is the number of packets that eavesdroppers can decode by collusion divided by the number of packets scheduled in a slot. By computing this over several runs, we identify the average exposed probability. This metric is shown in Figures 24 and 25 for the average and worst case respectively. One can observe that with 4 Access points and with 4 element arrays each, the average packet exposure ratio grows very gradually with increasing number of colluding eavesdroppers. Here we recall that collusion can only affect secret sharing,whereas controlled jamming and stream overwhelming would be unaffected by collusion. This explains why only with a large number of colluding eavesdroppers there is some increase in packet exposure ratio.i.e even with 25 colluding eavesdroppers the packet exposure ratio is less than 20%. However, from the worst case results, we obtain that as the number of eavesdroppers increases beyond the number of access points and antenna elements, the exposure ratio tends to 1. However, the results show a much

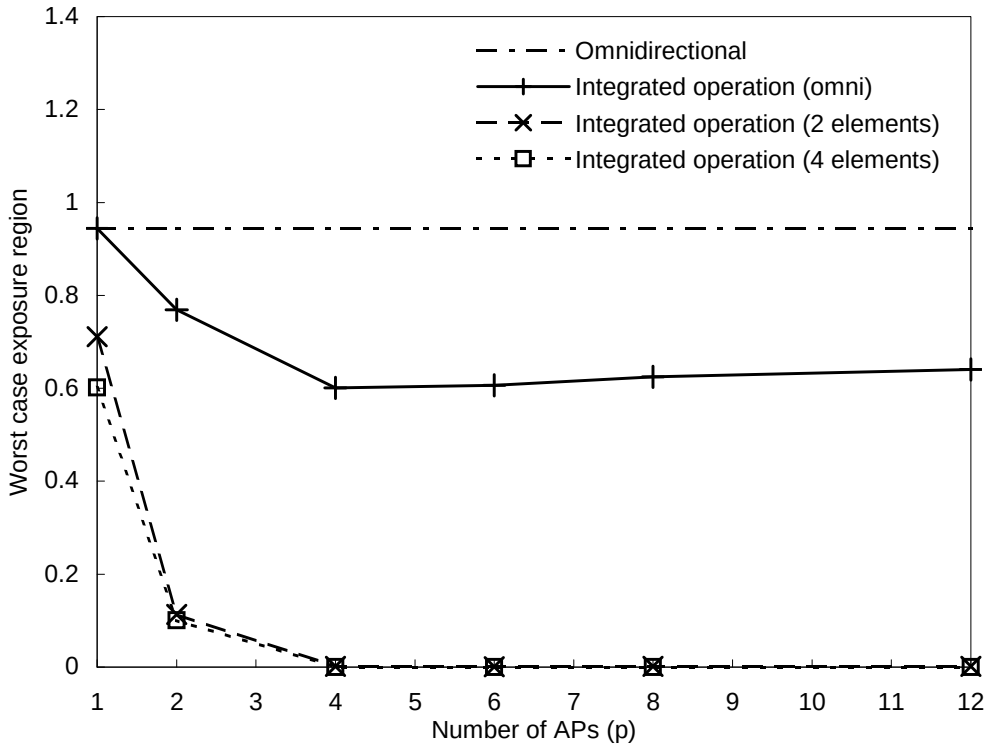

Figure 21: Impact of p - Worst case exposure region

gradual degradation in exposure ratio then in the case of simple beamforming. These results indicate the strength of the technique to eavesdropper capability.

5. Varying mobility of eavesdroppers:

As the eavesdroppers move, the algorithm would still work in the same manner as when the eavesdropper did not move. This is because, the algorithm does not assume any information about the mobility of the eavesdroppers. When the eavesdropper was allowed to move with a velocity from 5m/s to 20m/s, the security performance sees no significant change.

6. Throughput variation:

Although security is the main focus of the work, we are interested in exploring what throughput degradation will occur by using resources for security instead of throughput. The throughput results are shown in Figures 27 and 28. From the figures, one can conclude that the integrated algorithm is able to successfully ensure security

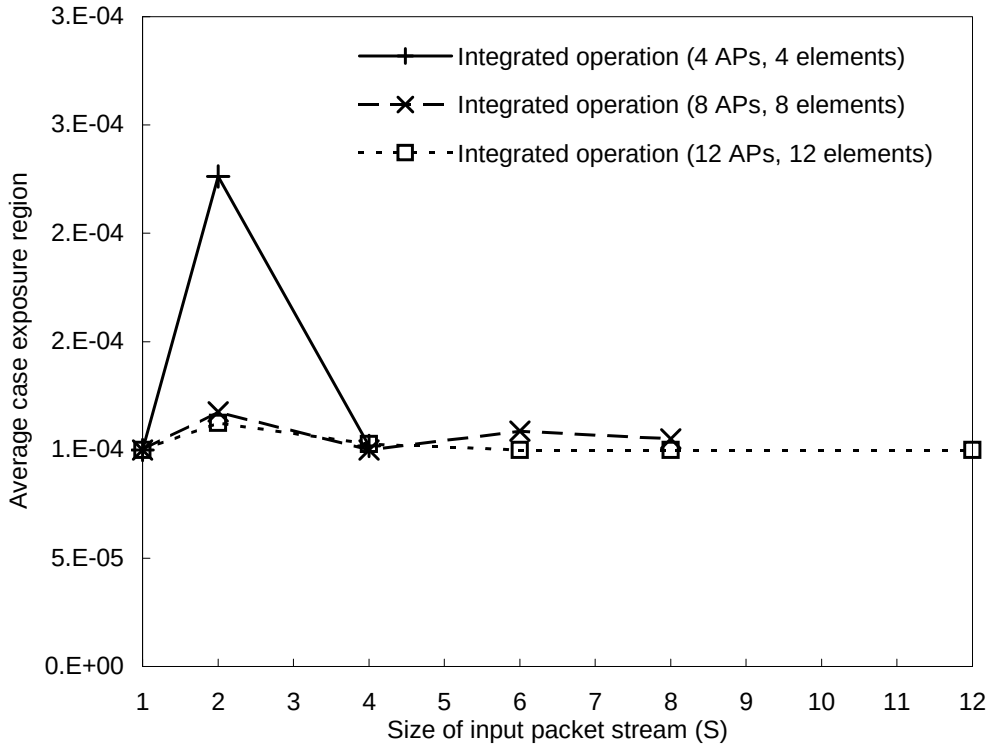

Figure 22: Variation of S - Average case

without any significant degradation in throughput. One can also observe that the network throughput saturates at a throughput value determined by the topology and number of nodes in the network. However, the general observation is that , for a fixed security level, the throughput increases with increasing antenna elements k or number of APs p since there are more resources available.

6.3 Proof of concept field trials

The objective of this section is to demonstrate that the proposed security solution can be applied to indoor environmental settings using minimal changes to off the shelf components. The field trials are carried out in the fifth floor of a high rise building 29. The equipment used consists of 4 commercial 802.11g (LINKSYS) broadband router equipped with two antennas and a laptop. The effect of beamforming is achieved by the use of a custom-built mechanical structure to provide a beamwidth of 60 degrees

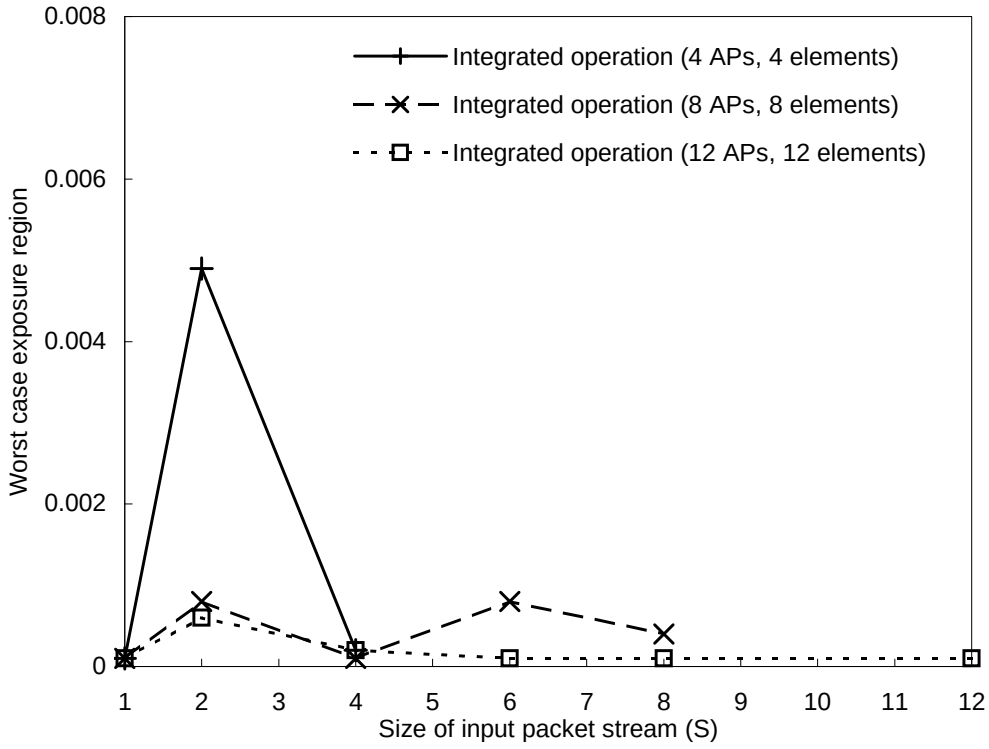

Figure 23: Variation of S - Worst case

and a mainlobe gain of 10 dB. 21 positions on the corridors of the building were identified for the experiment, with one client position and 20 as potential eavesdropper positions. The experiments conducted was the sending of ping packets from a laptop to the Access Point. The successful reception at any point is determined by the success of the ping packets. The table 1 shows the potential position in this setup, where an eavesdropper can decode the communication of an AP. Each row in the table represents the potential eavesdropper positions. A $\vee$ symbol indicates that it is possible to decode the signal successfully, whereas a "." symbol implies that the signal is not decodable. The second and third rows of the table show the points at which an eavesdropper can successfully decode the signal when the AP communicating to the client uses simple omni-directional antenna and a beamforming antenna respectively. The next two rows represent the points at which an eavesdropper can decode the signal when just secret sharing or secret sharing and controlled jamming is used as the

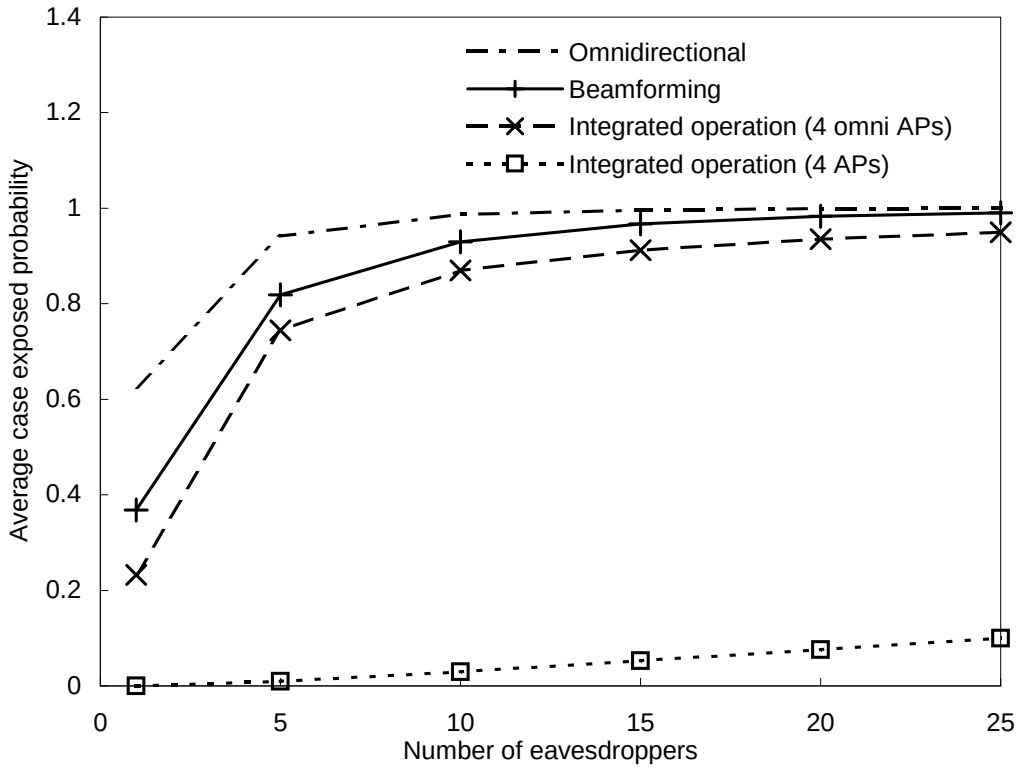

Figure 24: Eavesdropper collusion - Average case

strategy.It can be observed that the number of potential eavesdropper points is progressively reduced as each technique is applied and the maximum benefit is obtained using the integrated solution of beamforming+secret sharing+controlled jamming. The results show that although scattering exists, benefits are still obtainable in an indoor setting when the proposed solution is applied.

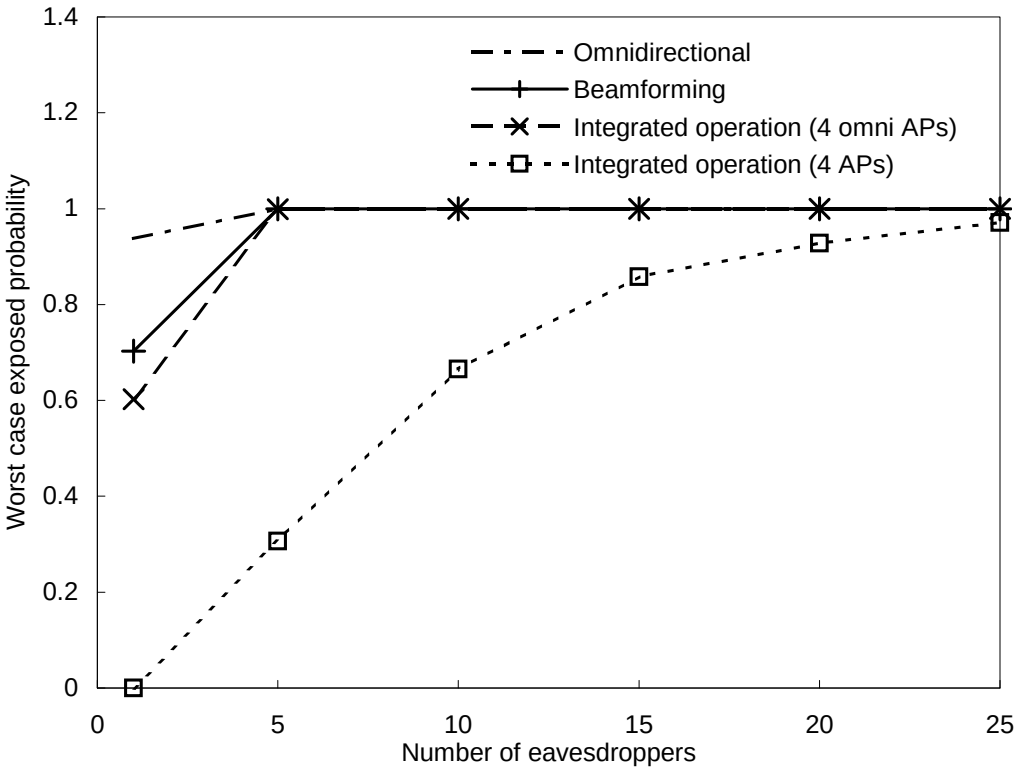

Figure 25: Eavesdropper collusion - Worst case

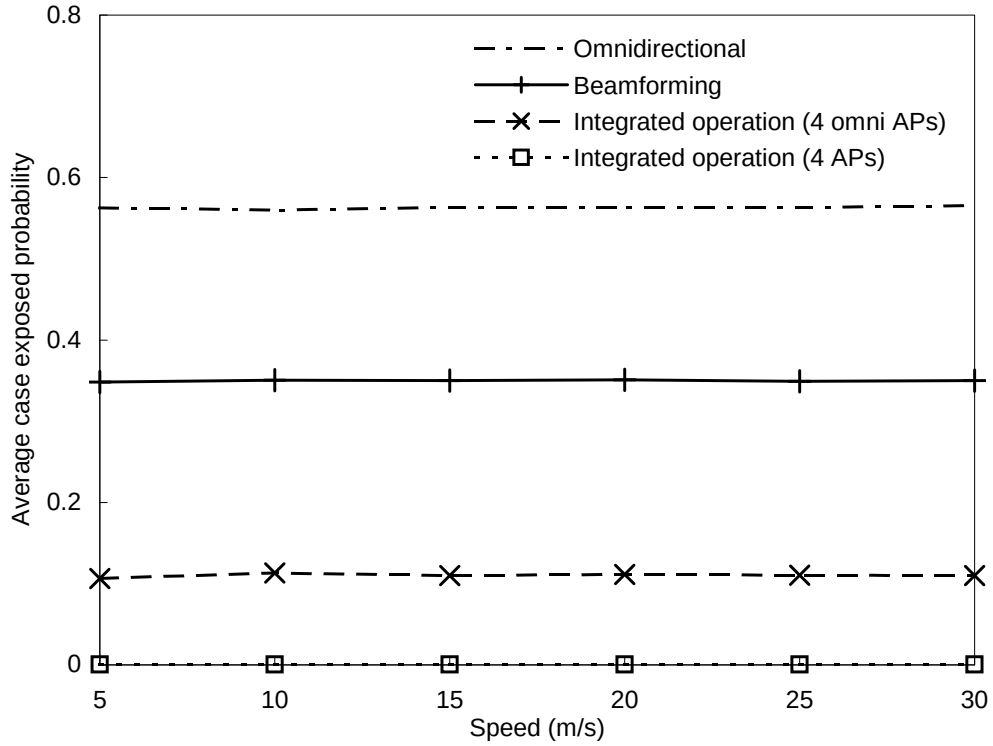

Figure 26: Impact of eavesdropper mobility

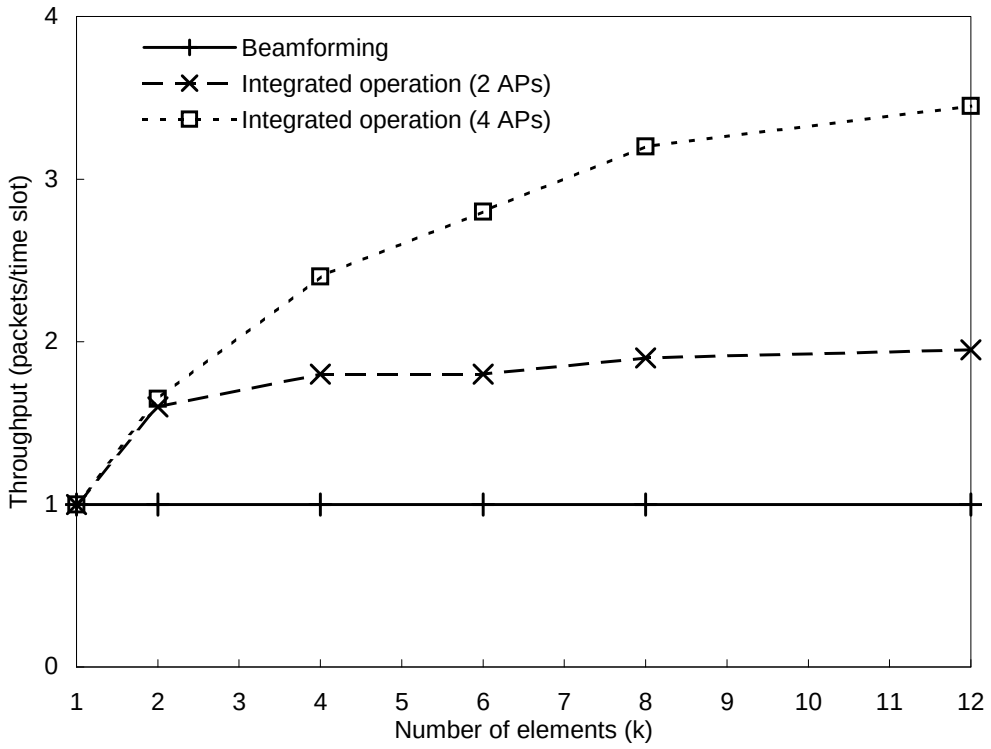

Figure 27: Throughput variation - Impact of k

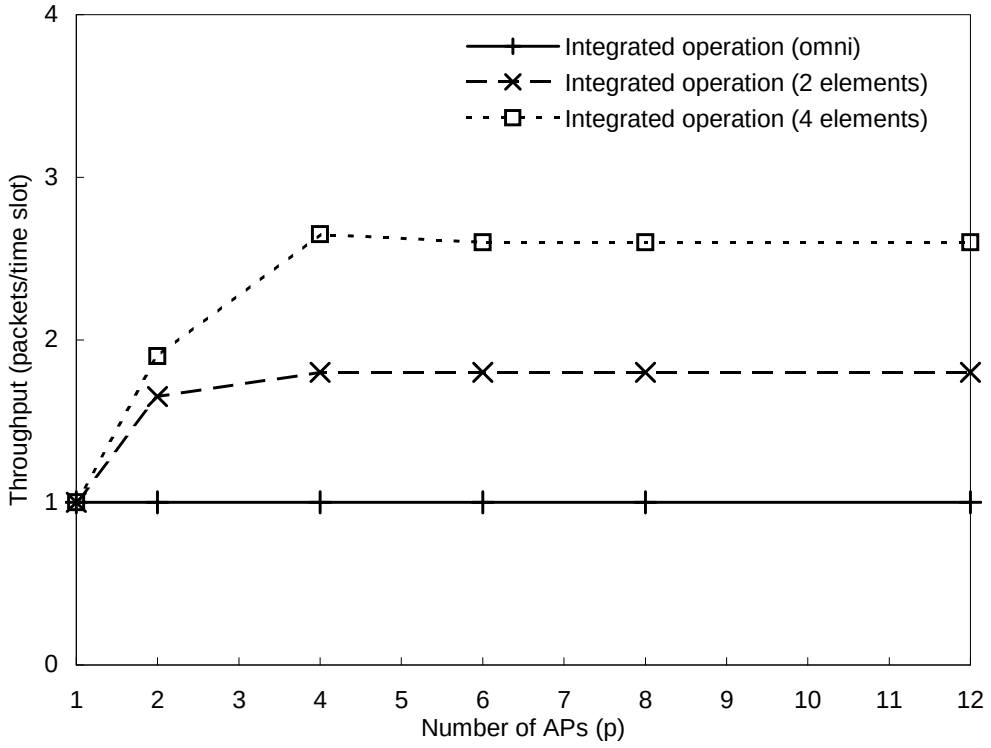

Figure 28: Throughput variation - Impact of p

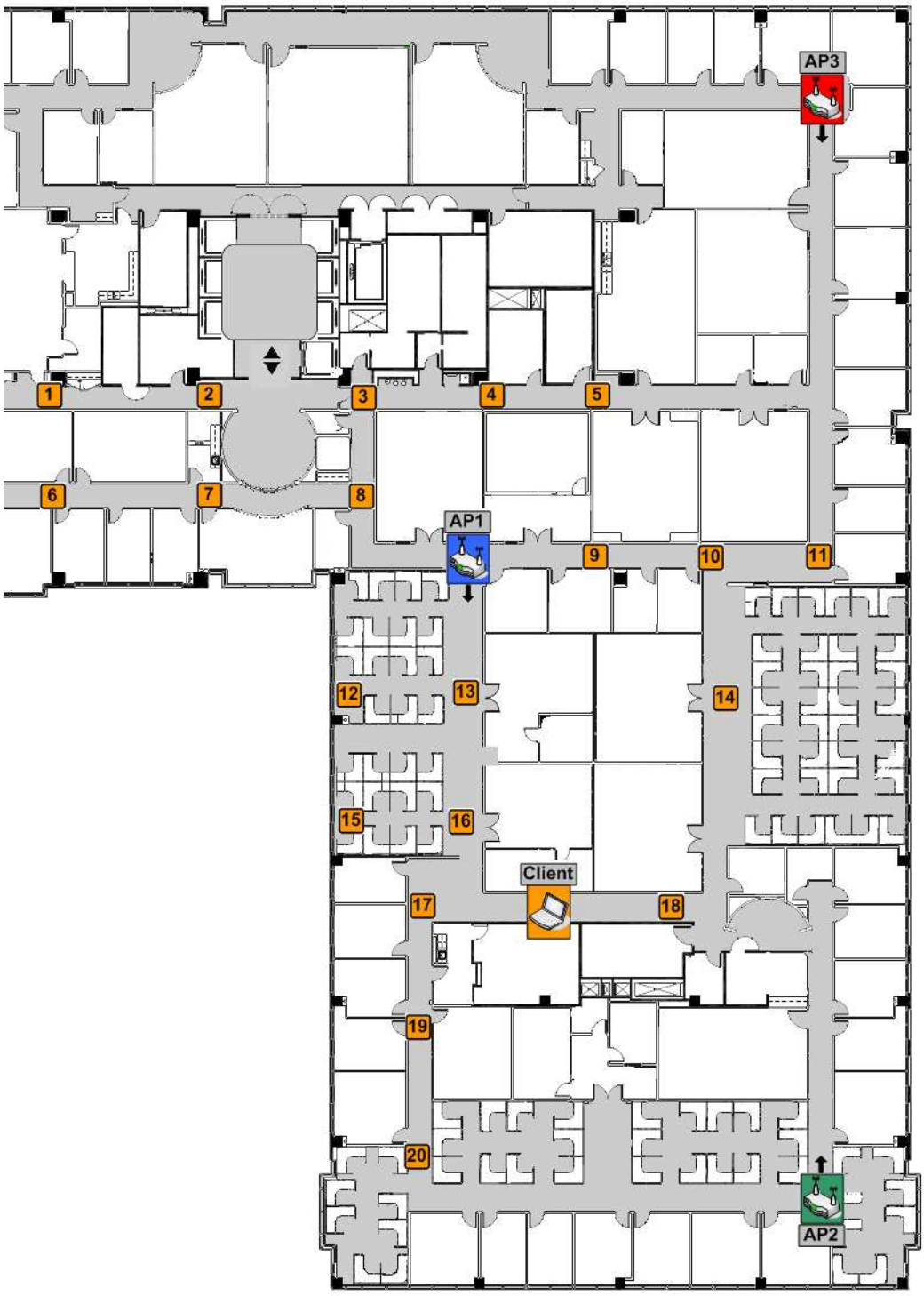

Figure 29: Floor map

Table 1: Field trials

Measurement Position	1	2	3	4	5	6	7	8	9	10	11
OMNI	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨	∨
BF	.	.	∨	∨	.	.	∨	∨	∨	∨	.
BF+SS	.	.	.	.	.	.	.	.	.	.	.
BF+CJ	∨	∨	∨	∨		∨	∨	∨	.	.	.
BF+SS+CJ	.	.	.	.	.	.	.	.	.	.	.

Measurement Position	12	13	14	15	16	17	18	19	20		Total
OMNI	∨	∨	∨	∨	∨	∨	∨	.	.		18
BF	∨	∨	∨	∨	∨	∨	.	∨	∨		14
BF+SS	.	.	∨	.	.	∨	.	∨	∨		4
BF+CJ	∨	∨	.	∨	∨	∨	.	∨	∨		14
BF+SS+CJ	.	.	.	.	.	∨	.	∨	∨		3

CHAPTER VII

RELATED WORKS

The security problems in WLANs have been well documented in [10, 7, 24]. There are also several solutions to specific problems in WLAN but all such works are purely higher layer cryptographic mechanisms [9, 25]. In fact standardization of security techniques for wireless LANs has also been accomplished in the form of IEEE 802.11i [12]. In [17], the authors propose a shared key strategy that generates and extract keys from channel state information. In rich scattering environment, the eavesdropper experiences different channel because of high decorrelation from the sender-receiver path, and as a result it extracts a different key. In [13], the authors describe how the signal strength information called signalprint can be exploited to prevent malicious transmitter from attacking the wireless network such as denial-of-service. Based on the fact that the signalprints are strongly correlated with the clients' location, the proposed scheme detects and tags suspicious packets. In both the above examples, the authors do not consider smart antennas and the goals are different.

In [23], the authors propose an authentication scheme that uses dual smart antennas. In this paper, an adaptive beam-forming antenna is used to identify and locate the legal user through receiving the authentication packets (called antenna ID authentication), and a switched multiple-beam antenna is used for transmissions of data packets. The focus of this work is orthogonal to the one in this paper. Another security technique is described in [11], where the authors discuss spatial data striping techniques that increase the degree of security using a phased array antenna in 802.11 environments. However no algorithms or solution details are provided, and no specific

security metrics are considered or evaluated. In [19], the authors describe a theoretical communication scheme in which coding using the multiple degrees of freedom is used to generate "artificial noise", which degrades only the eavesdropper's channel quality. Again, the paper does not provide any protocol or solution details, requires strict channel synchronization, and does not consider the eavesdropper equipped with smart antennas.

CHAPTER VIII

CONCLUSION AND FUTURE WORK

8.1 Conclusion

In sum, the idea of using spatial smartness to provide security against eavesdropping was introduced. Specifically, the security implications of using smart antennas were described in the context of a WLAN , using the abstraction of a virtual array of physical arrays. Three novel mechanisms that fundamentally improve security against eavesdropping were described and their benefits quantified through extensive simulations. Further, the trade-offs in the use of the three schemes were highlighted and a greedy algorithm to obtain a the highest integrated benefit was described. The performance of the algorithm was evaluated using simulations. Finally, we believe that this is the first solution that uses capability of smart antennas at higher layers for security. Significant gains over both omni-directional and simple beamforming techniques indicate the power of the mechanisms. Although we have provided three novel mechanisms, a more complete exploration of the trade-offs and the optimal benefits achievable are part of future work.

8.2 Future work

In this section, we briefly discuss a few issues that pertain to the approaches presented in the thesis thus far. We believe that these are important issues, but can be addressed as part of future research with this work forming the basis.

Scattering effects: In the presence of scattering, signals arrive at the receiver from multiple paths with varying amplitude and phases. Weight adaptation is the primary technique used in beamforming to tackle scattering. While the total area of the beam

will not change with adapted weights, the shapes of the beams do change. We contend that the as long as the angular spread is not very large, benefits outlined in this work are still good approximations of achievable security. In the event that the angular spread is large, one possible solution is to use a learning process with the cooperation of other legal clients to understand coarse-level characteristics of the scattering, and use this information in the scheduling algorithms.

3-D model: We have used a 2-D model for the area of exposure in this work, which results in an area of interest. We believe that extending the results and the algorithms to a 3-D model that considers volume of exposure is possible in a straightforward manner. Perhaps more importantly, the security benefits demonstrated thus far *can be expected to increase* when a 3-D model is adopted as the benefits of smart antennas will now be raised to a larger exponent.

Multiple associations and co-channel APs: This work makes two assumptions about multiple client associations and multiple co-channel APs. While current WLANs operate on different channels to reduce interference, the proliferation of WLANs and the limited number of available channels, has already lead to multiple co-channel APs naturally co-existing in a single channel [5]. Furthermore, with smart antennas it is possible to sustain multiple co-channel transmissions in a given region justifying the choice even further. Further, while multiple AP associations for a client is not currently enabled due to ease of identifying downstream clients through their associated APs, this requirement does not have a fundamental basis and is likely to change since multiple associations has other benefits such as diversity and capacity as well.

Effects of client mobility: While we considered eavesdropper mobility in the performance evaluation, we have not considered client mobility thus far. It can be argued that the only impact client mobility will have on the proposed solutions is in terms of how fast the location information of the clients can be fed back to the controller. Even in the presence of location errors, because of the controller's assumption of a

link margin, the performance should still not suffer. Furthermore, since decisions of the controller are taken at a per slot level, and mobility of clients is likely to occur at much coarser granularities, very minimal impact is likely to be experienced by the algorithms presented.

REFERENCES

[1] "IEEE 802.11n: WLAN MAC and PHY Specifications..", *http://ieee.standards.org*, September 20 2007.

[2] "IEEE 802.16: Broadband Wireless Metropolitan Area Networks.", *http://ieee.standards.org*, September 20 2007.

[3] "Ruckus Wireless inc..", *http://www.ruckuswireless.com*, September 20 2007.

[4] W. JACKSON.,"Cracks in the air:justice security expert shows how easy it can be to defeat wireless security," Available online at *http://www.gcn.com/print/26_10/44213-1.html*, September 20 2007.

[5] AKELLA, A., JUDD, G., STEENKISTE, P., and SESHAN, S., "Self management in chaotic wireless deployments," in *ACM Conference on Mobile Computing and Networking (MOBICOM)*, Sept. 2005.

[6] A.PAULRAJ, R.NABAR, and D.GORE, "Introduction to space-time wireless communications," *Cambridge University Press*, May 2003.

[7] ARBAUGH, W. A., SHANKAR, N., WAN, Y. C. J., and ZHANG, K., "Your 802.11 wireless network has no clothes," *IEEE Wireless Communications Magazine*, vol. 10, pp. 8–14, Oct. 2003.

[8] A.SHAMIR, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[9] BAHL, P., CHANDRA, R., PADHYE, J., RAVINDRANATH, L., SINGH, M., WOLMAN, A., and ZILL, B., "Enhancing the security of corporate wi-fi networks using DAIR," *ACM MOBISYS* 2006 .

[10] BORISOV, N., GOLDBERG, I., and WAGNER, D., "Intercepting mobile communications: the insecurity of 802.11," in *ACM Conference on Mobile Computing and Networking (MOBICOM)*, pp. 180–189, July 2001.

[11] CAREY, J. M. and GRUNWALD, D., "Enhancing wlan security with smart antennas: A physical layer response for information assurance," in *IEEE Vehicular Technology Conference (VTC)*, vol. 1, pp. 318–320, Sept. 2004.

[12] CHEN, J.-C., JIANG, M.-C., and LIU, Y.-W., "Wireless LAN security and IEEE 802.11i," *IEEE Wireless Communications*, vol. 12, pp. 27–36, Feb. 2005.

[13] FARIA, D. B. and CHERITON, D. R., "Detecting identity-based attacks in wireless networks using signalprints," *ACM Wireless Security Workshop (WiSe)*, pp. 43–52, Sept. 2006.

[14] Fitzgerald, J., *Business Data Communications*. John Wiley and sons, 1984.

[15] J.Mailloux, R., *Phased Array Antenna Handbook*. Artech House, 1993.

[16] J.Stallings, W., *Cryptography and Network Security, Third Edition*. Prentice Hall inc., 2003.

[17] Li, Z., Xu, W., Miller, R., and Trappe, W., "Securing wireless systems via lower layer enforcements," *ACM Wireless Security Workshop (WiSe)*, pp. 33–42, Sept. 2006.

[18] Mishra, A., Agrawal, D., Shrivastava, V., Banerjee, S., and Ganguly, S., "Distributed channel management in uncoordinated wireless environments," in *ACM International Conference on Mobile Computing and Networking (MOBICOM)*, Sept. 2006.

[19] Negi, R. and Goel, S., "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference (VTC)*, vol. 3, pp. 1906–1910, Sept. 2005.

[20] Pang, J., Greenstein, B., Gummadi, R., Seshan, S., and Wetherall, D., "802.11 User fingerprinting," in *ACM Conference on Mobile Computing and Networking (MOBICOM)*, Sept. 2007.

[21] Richards, M., *Fundamentals of Radar Signal Processing*. McGraw Hill inc., 2005.

[22] Rivest, R. L., "All-or-nothing encryption and the package transform," *Lecture Notes in Computer Science*, vol. 1267, p. 210, 1997.

[23] Sun, Z. and Lu, J., "Improving the security performance in mobile wireless computing network using smart directional antenna," in *IEEE Asia-Pacific Conference on Environmental Electromagnetics (CEEM)*, pp. 47–50, Nov. 2003.

[24] Wagner, D., Schneier, B., and Kelsey, J., "Cryptoanalysis of the cellular encryption algorithm," in *International Cryptology Conference on Advances in Cryptology (CRYPTO)*, (London, UK), pp. 526–537, 1997.

[25] Yeo, J., Youssef, M., and Agrawala, A., "A framework for wireless LAN monitoring and its applications," *ACM Wireless Security workshop (WiSe)*, pp. 70–79, 2004.